



天锐绿盾桌面管理系统 管理员使用手册

厦门天锐科技股份有限公司

版权声明

本文件以及所提及的数据、图标、名称、所有权皆属于厦门天锐科技股份有限公司所有。未得到厦门天锐科技股份有限公司的书面认可，任何个人或组织均不得以任何手段与形式对本方案内容进行复制、转印和传播。

本文件中的内容，厦门天锐科技股份有限公司拥有最终解释权。



目 录

| | |
|----------------------|----|
| 目 录 | I |
| 1 前言 | 1 |
| 2 系统使用 | 1 |
| 2.1 系统运维 | 1 |
| 2.1.1 终端信息 | 1 |
| 2.1.2 进程管理 | 2 |
| 2.1.3 资源管理器 | 3 |
| 2.1.4 软件管理 | 4 |
| 2.1.4.1 软件信息 | 4 |
| 2.1.4.2 创建卸载任务 | 7 |
| 2.1.4.3 任务分发情况 | 10 |
| 2.1.5 软件卸载记录 | 11 |
| 2.1.5.1 实时卸载记录 | 11 |
| 2.1.5.2 任务操作记录 | 12 |
| 2.1.5.3 任务分发记录 | 13 |
| 2.1.6 设备管理 | 14 |
| 2.1.7 系统服务 | 14 |
| 2.1.8 共享管理 | 15 |
| 2.1.8.1 查看共享列表 | 15 |
| 2.1.8.2 配置共享策略 | 16 |
| 2.1.9 远程协助 | 16 |
| 2.1.10 远程控制 | 18 |
| 2.2 策略管理 | 19 |
| 2.2.1 应用程序限制 | 19 |
| 2.2.1.1 程序限制 | 19 |
| 2.2.1.2 窗口限制 | 20 |
| 2.2.1.3 软件版本限制 | 22 |
| 2.2.2 应用程序分类管理 | 24 |
| 2.2.3 软件安装包限制 | 26 |
| 2.2.3.1 策略总览 | 27 |
| 2.2.3.2 安装限制 | 28 |
| 2.2.3.3 卸载限制 | 29 |
| 2.2.3.4 特殊目录放行 | 30 |
| 2.2.3.5 终端上报程序 | 31 |
| 2.2.4 打印水印设置 | 32 |
| 2.2.4.1 配置信息列表 | 32 |
| 2.2.4.2 受控程序 | 35 |
| 2.2.5 移动存储管理 | 36 |
| 2.2.5.1 USB 存储设备限制 | 36 |
| 2.2.5.2 USB 存储设备认证 | 37 |
| 2.2.5.3 USB 存储设备接入审批 | 43 |
| 2.2.6 硬件设备控制 | 44 |
| 2.2.7 网站/网页内容限制 | 45 |



| | |
|-----------------------|----|
| 2.2.7.1 网站限制..... | 46 |
| 2.2.7.2 网页内容限制..... | 48 |
| 2.2.8 聊天工具白名单..... | 49 |
| 2.2.9 聊天工具文件控制..... | 50 |
| 2.2.10 网络流量限制..... | 51 |
| 2.2.11 网络端口限制..... | 56 |
| 2.2.12 局域网网段限制..... | 57 |
| 2.2.13 IP/MAC 绑定..... | 58 |
| 2.2.14 ARP 防火墙设置..... | 59 |
| 2.2.15 网络隔离设置..... | 60 |
| 2.2.16 邮件内容限制..... | 63 |
| 2.3 资产管理..... | 64 |
| 2.3.1 资产变更报警设置..... | 64 |
| 2.3.2 硬件资产..... | 64 |
| 2.3.3 硬件资产变更记录..... | 66 |
| 2.3.4 硬件资产变更报警..... | 67 |
| 2.3.5 软件资产..... | 68 |
| 2.3.6 软件资产变更记录..... | 69 |
| 2.3.7 软件资产变更报警..... | 70 |
| 2.4 任务推送..... | 71 |
| 2.4.1 文件分发..... | 71 |
| 2.4.1.1 上传分发文件..... | 71 |
| 2.4.1.2 创建并分配任务..... | 73 |
| 2.4.2 分发日志..... | 74 |
| 2.4.2.1 执行任务..... | 74 |
| 2.4.2.2 历史任务..... | 76 |
| 2.5 补丁管理..... | 76 |

1 前言

天锐绿盾桌面管理系统（简称：桌面管理系统）实现终端桌面的标准化管理，解决桌面安全管理问题，提升信息运行维护部门的工作效率，同时规范员工操作行为。

桌面管理系统由客户端、服务端、控制台三部分组成。客户端对终端计算机进行管控，部署在每台需要管理的终端计算机上，用于收集数据信息，并执行来自服务端下发的指令。服务端存储终端安全策略、终端资产信息、软件分发信息等等，并由服务端向终端计算机发送指令。控制台用来管控所有终端计算机，并制定相关安全策略。

其中 Windows 终端支持以下介绍的所有功能，Mac 终端目前支持远程协助、移动存储管理、网络端口限制和 IP/Mac 绑定功能。

2 系统使用

2.1 系统运维

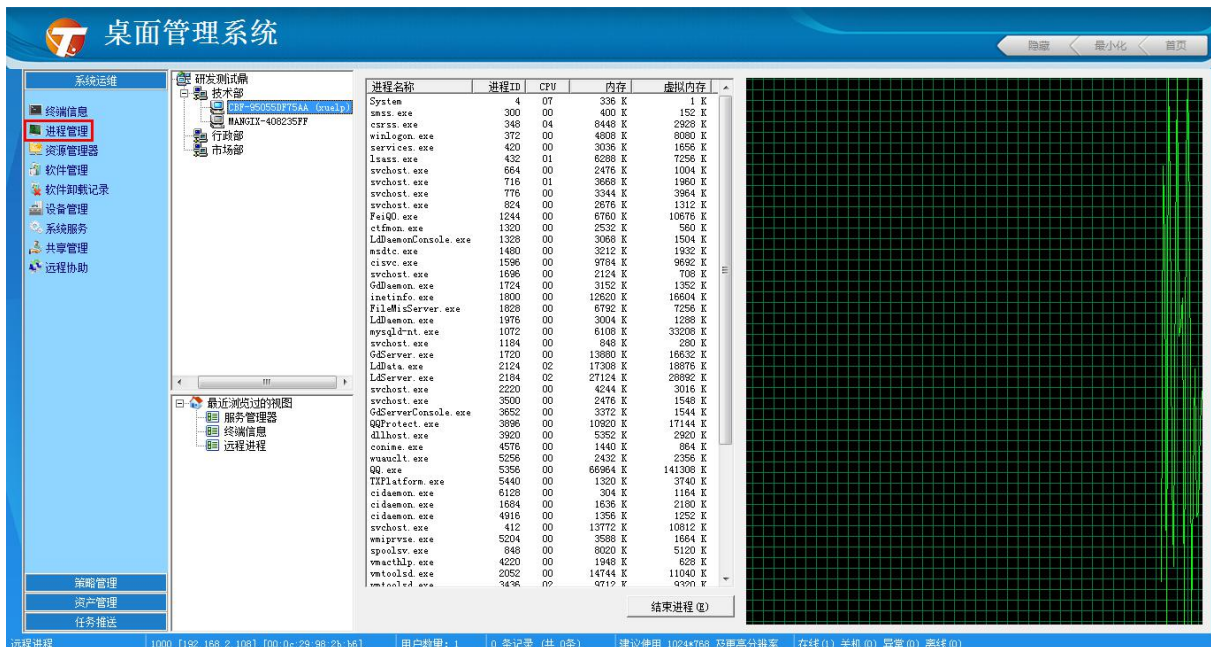
2.1.1 终端信息

查看终端编号、终端名称、终端计算机名称、操作系统、开机时间、系统用户、IP、MAC 地址、磁盘信息、系统性能等信息。在控制台的功能栏选择“系统运维”-“终端信息”，用户列表栏选择要查看的用户，详细信息栏将显示该终端当前的信息情况，显示的内容包括终端电脑的基础信息、磁盘信息、系统信息和 CPU 使用情况。如下图所示：



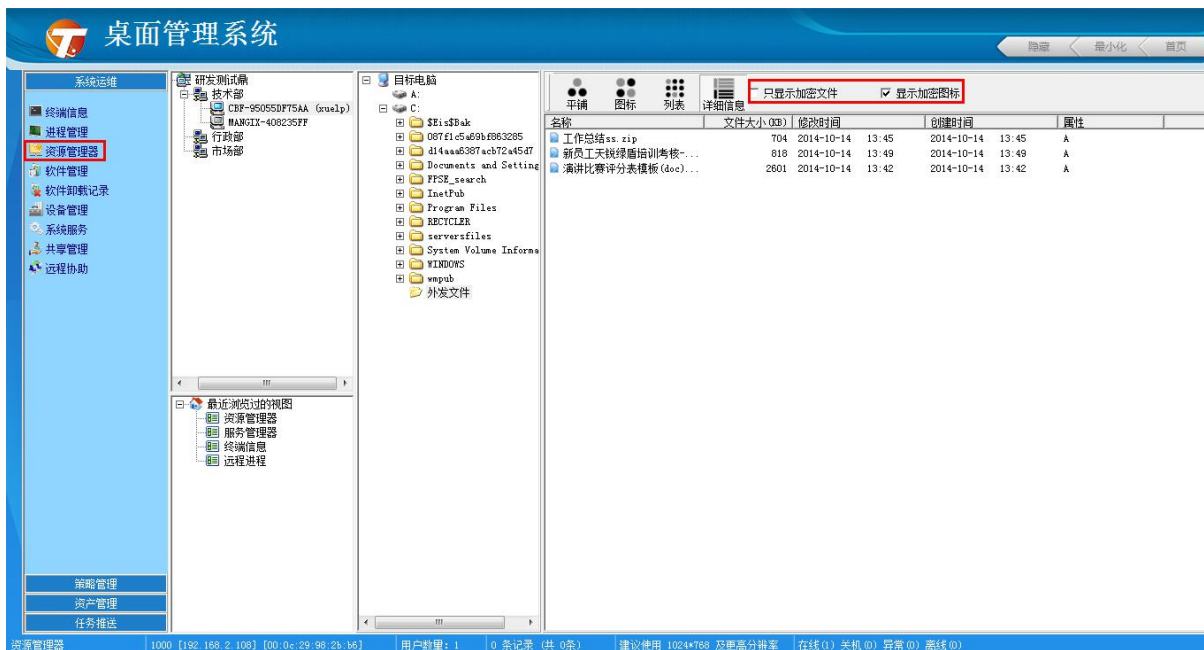
2.1.2 进程管理

在控制台的功能栏选择“系统运维”-“进程管理”，用户列表栏选择要查看的用户，详细信息栏将显示该终端当前的进程列表，显示的列包括进程名称、进程 ID、CPU 使用率、内存、虚拟内存。选中指定进程，再点击“结束进程”按钮，可以远程结束进程。如下图所示：

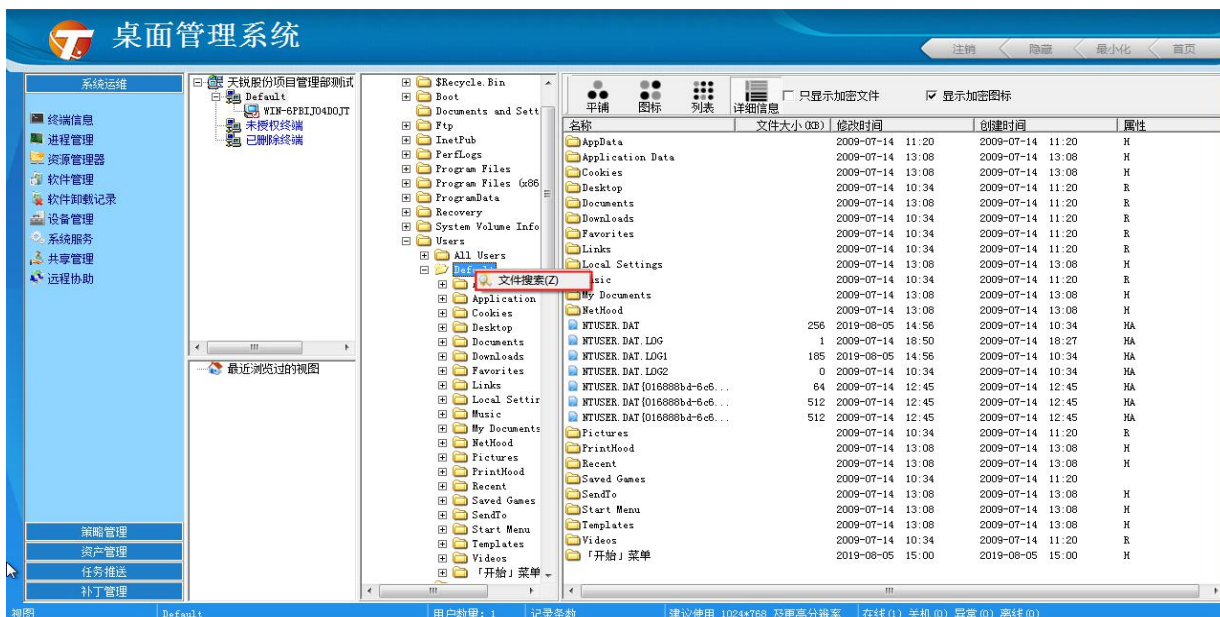


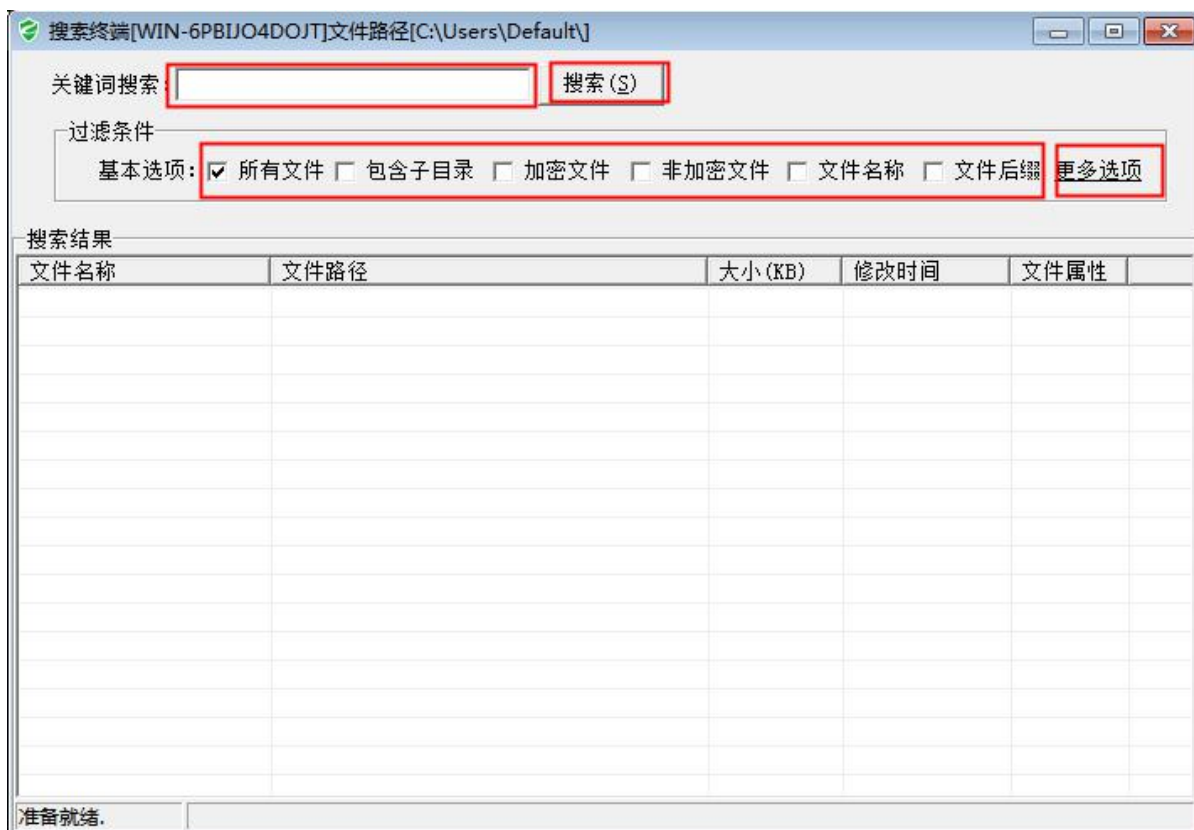
2.1.3 资源管理器

在控制台的功能栏选择“系统运维”-“资源管理器”，用户列表栏选择要查看的用户，详细信息栏可以列出选定终端当前电脑硬盘的资源情况，可选择只显示加密文件，且加密文件显示加密图标。资源文件只可查看，无法修改、删除。如下图所示：



用户列表栏选择要查看的用户，详细信息栏选中盘符或者文件夹右键点击“文件搜索”，弹出搜索框，点击“更多选项”即可下拉出更多的过滤条件，自定义搜索条件点击“搜索”即可查出目标文件。（注意：当搜索文档时，所选的文件夹中包含子文件夹需要勾选“包含子目录”+检索条件方可快速搜索出对应文档）

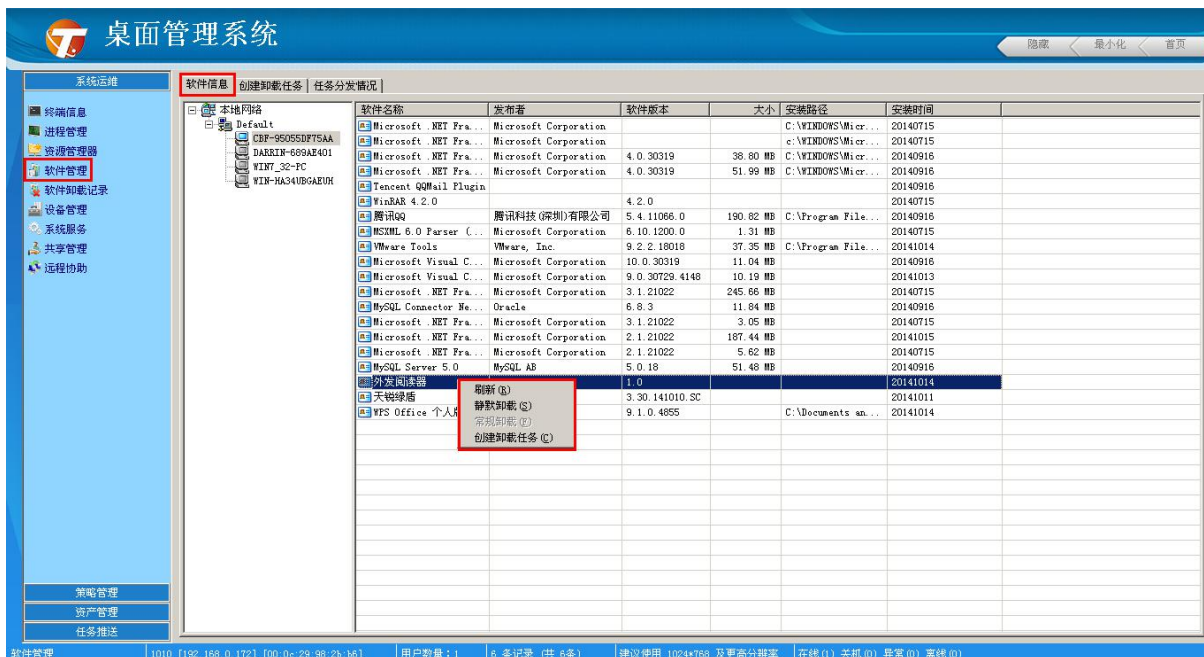




2.1.4 软件管理

2.1.4.1 软件信息

查看终端电脑已安装的软件清单，支持从控制台远程卸载指定的软件。在控制台的功能栏选择“系统运维”-“软件管理”-“软件信息”，用户列表栏选择要查看的终端用户，详细信息栏将显示终端电脑已安装的软件清单。可以远程卸载软件，卸载方式包括静默卸载和常规卸载，也可以通过任务分发的方式，进行批量卸载。如下图所示：



常规、静默卸载

常规卸载要软件程序本身能够支持，静默卸载可以支持大部分的软件卸载。采用静默卸载时，系统会自动搜索跟要卸载的软件相关的安装信息，用户来确认选择要删除的文件或文件夹。

注意：静默卸载方式可能会引起系统不稳定，请谨慎使用。

创建卸载任务

鼠标右键某一软件，选择“创建卸载任务”菜单，弹出“创建卸载任务”窗口，在“任务名”和“备注”栏处输入相应数据，并选择卸载方式（**说明：**要卸载的软件本身支持常规卸载时才可以选择常规卸载，否则显示为“灰色”不能操作）。选择静默卸载时，可以设置卸载时不删除指定文件或文件夹。如下图所示：

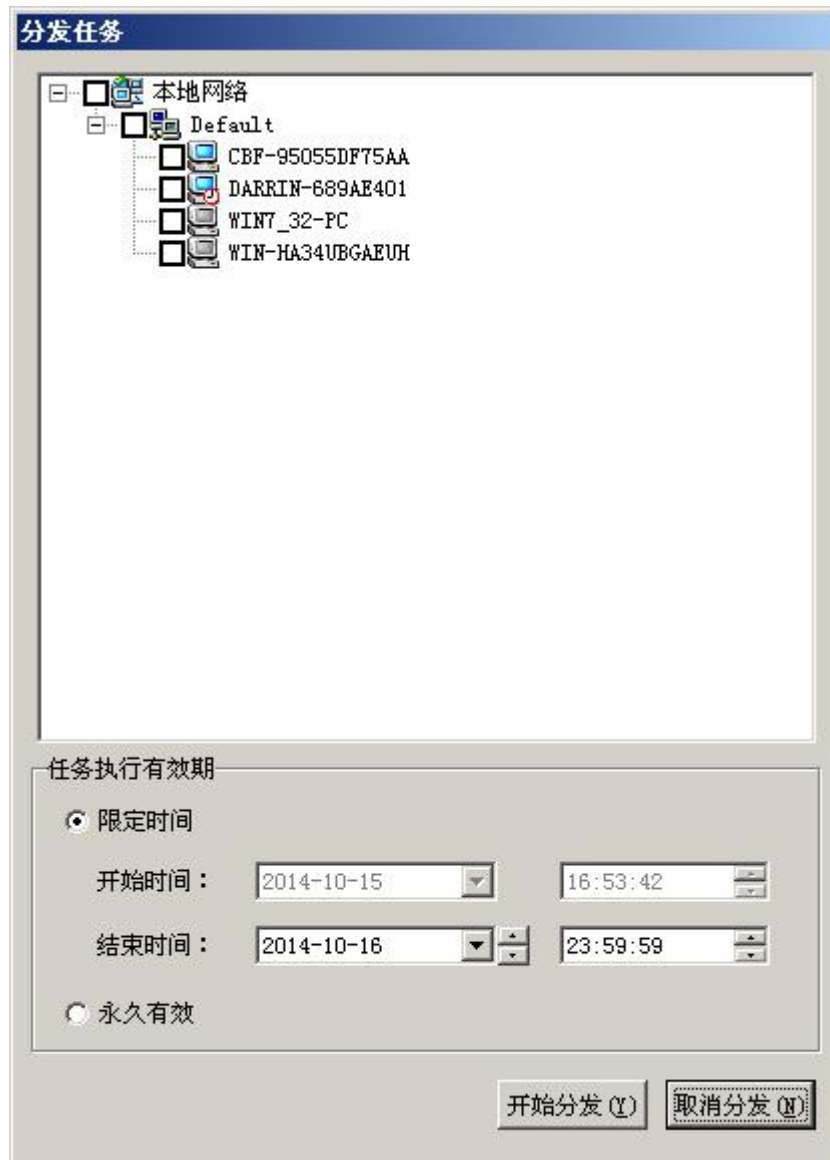


设置完成后，点击“确定”按钮，弹出“系统提示”窗口，根据需要选择是否要马上分发卸载任务。如下图所示：



需要马上分发任务，则点击“确定”按钮，弹出“分发任务”窗口，选择任务要分发的对象，设置任务执行的有效期。设置完成后，点击“开始分发”按钮即可。

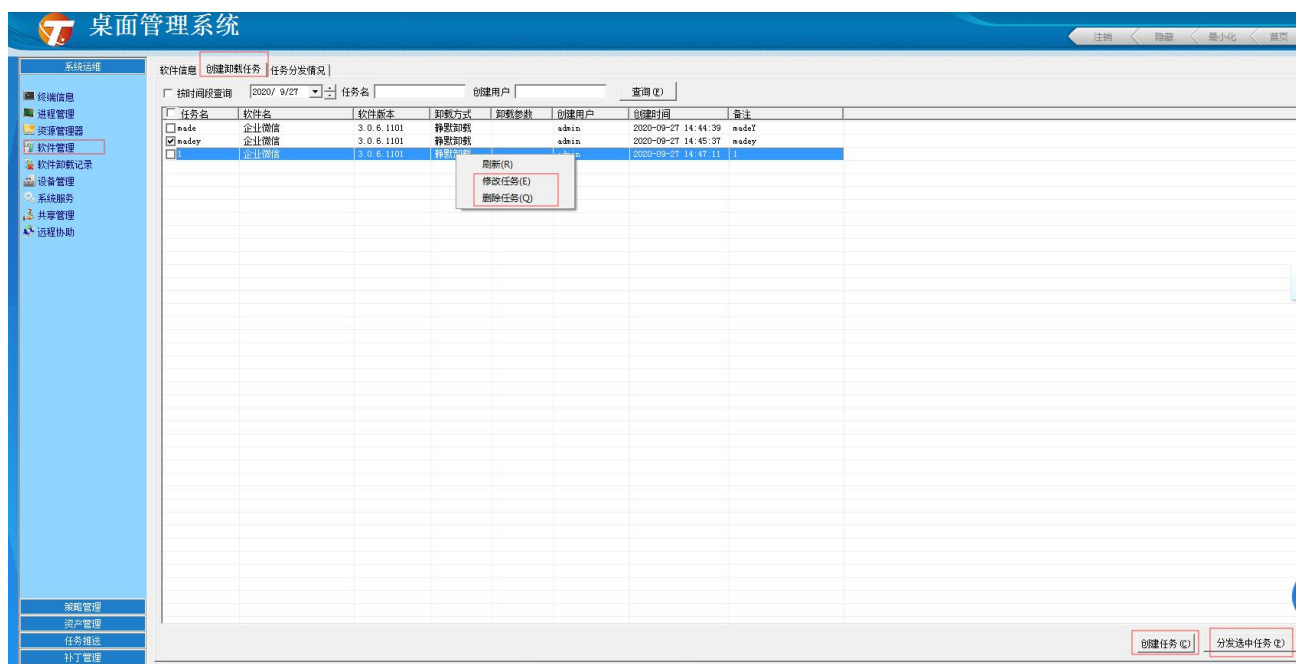
如果选择“取消”按钮，下次需要对任务进行分发时，在“创建分发任务”窗口的任务列表中，先选择要分发的任务，然后点击“分发选择任务”按钮，在弹出“分发任务”窗口进行设置。如下图所示：



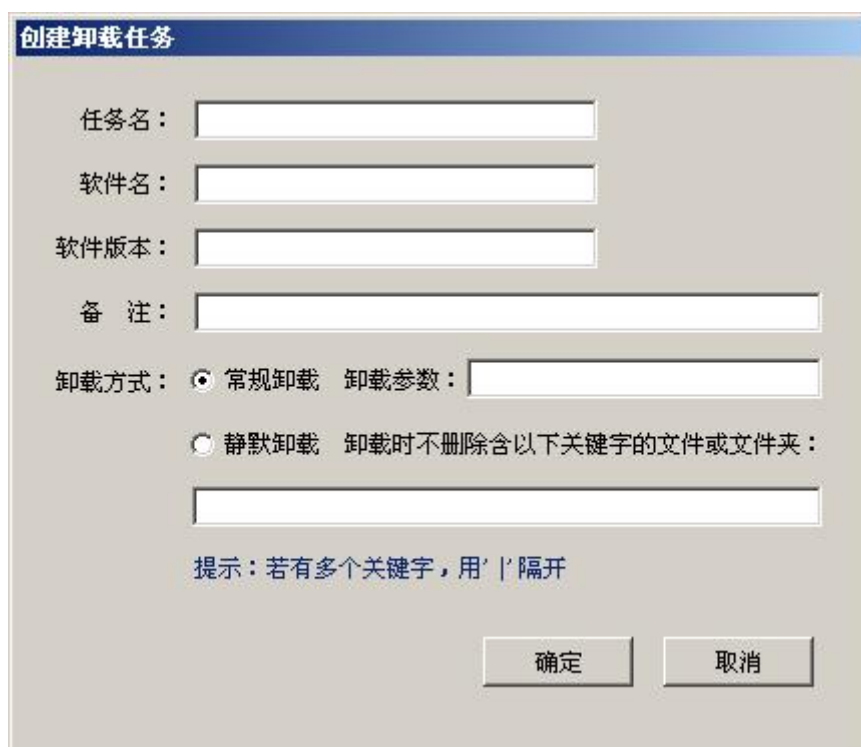
注意：卸载任务还没有分发时，不会进行卸载操作。

2.1.4.2 创建卸载任务

可以在“软件信息”页面直接创建该软件的卸载任务，也可以在“创建卸载任务”页面中创建其他软件的卸载任务。在控制台的功能栏选择“系统运维”-“软件管理”-“创建卸载任务”，如下图所示：



点击“创建任务”按钮，弹出“创建任务”窗口，在“任务名”、“软件名”、“软件版本”和“备注”栏处输入正确的数据，并选项卸载方式。选择静默卸载时，可以设置卸载时不删除指定的文件和文件夹。如下图所示：



创建卸载任务

任务名：

软件名：

软件版本：

备 注：

卸载方式： ☒ 常规卸载 卸载参数：

☐ 静默卸载 卸载时不删除含以下关键字的文件或文件夹：

提示：若有多个关键字，用'|'隔开

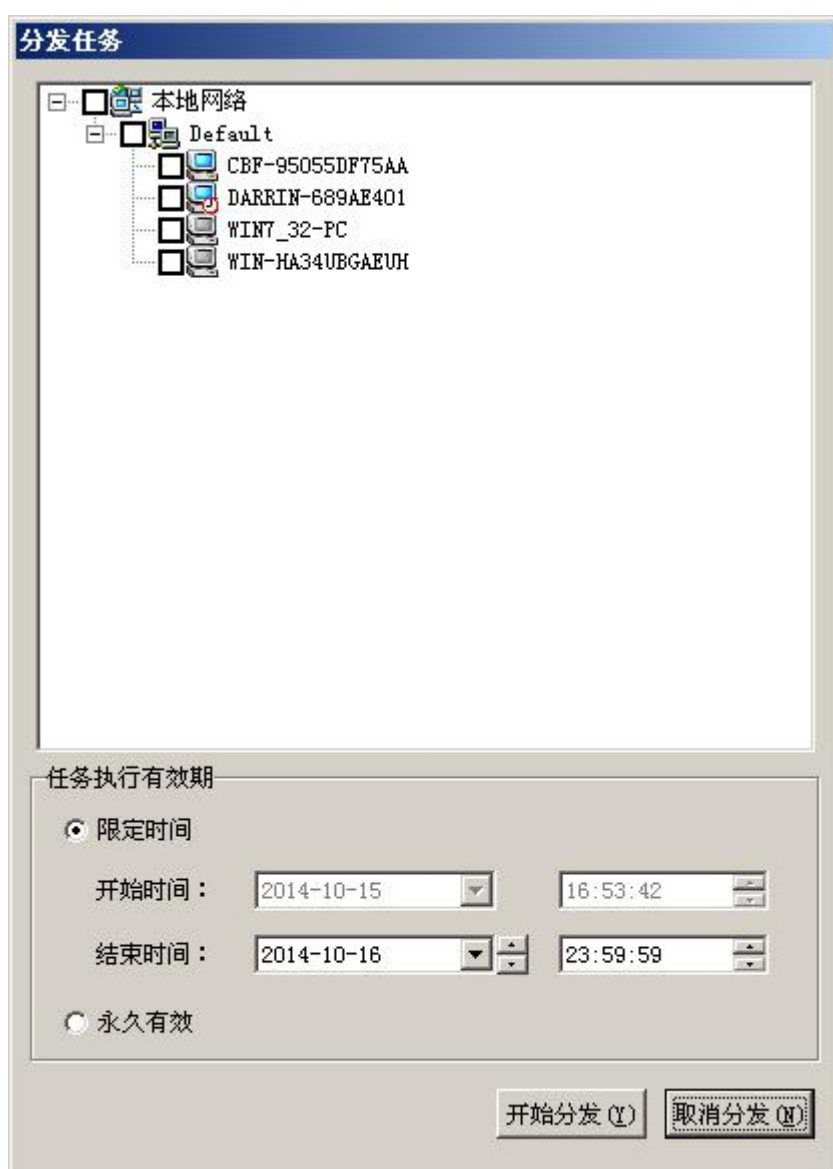
确定 取消

设置完成后，点击“确定”按钮，弹出“系统提示”窗口，根据需要选择是否要马上分发卸载任务。如下图所示：



需要马上分发任务，则点击“确定”按钮，弹出“分发任务”窗口，选择任务要分发的对象，设置任务执行的有效期。设置完成后，点击“开始分发”按钮即可。

如果选择“取消”按钮，下次需要对任务进行分发时，在“创建分发任务”窗口的任务列表中，先选择要分发的任务，然后点击“分发选择任务”按钮，在弹出“分发任务”窗口进行设置。如下图所示：

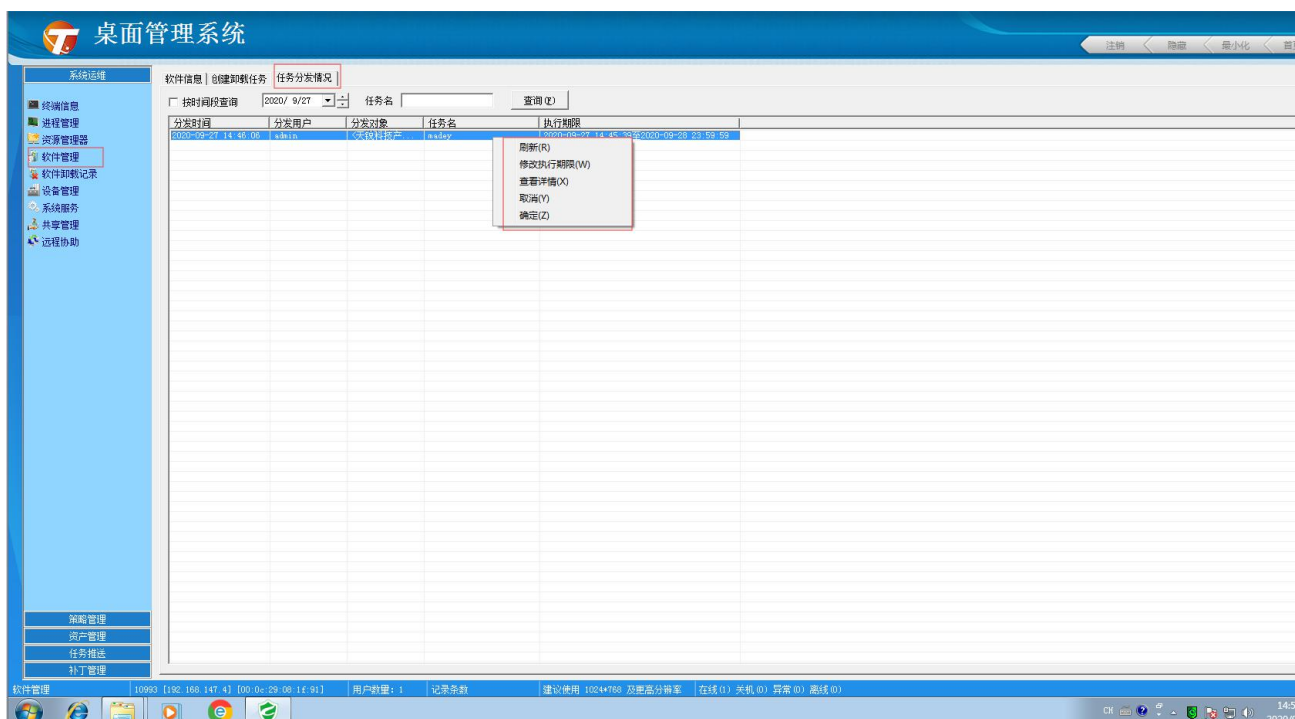


可以修改、删除卸载任务。鼠标右键任务，选择“修改任务”或“删除任务”菜单进行操作。**注意：**任务在分发状态时，无法进行修改。可以在“任务分发情况”窗口中，将该任务取

消后，再进行修改。

2.1.4.3 任务分发情况

查看任务分发情况，包括任务执行有效期、是否过期、任务分发详情等，可以修改任务执行有效期。另外可以设置任务完成或取消任务。在控制台的功能栏选择“系统运维”-“软件管理”-“任务分发情况”，如下图所示：

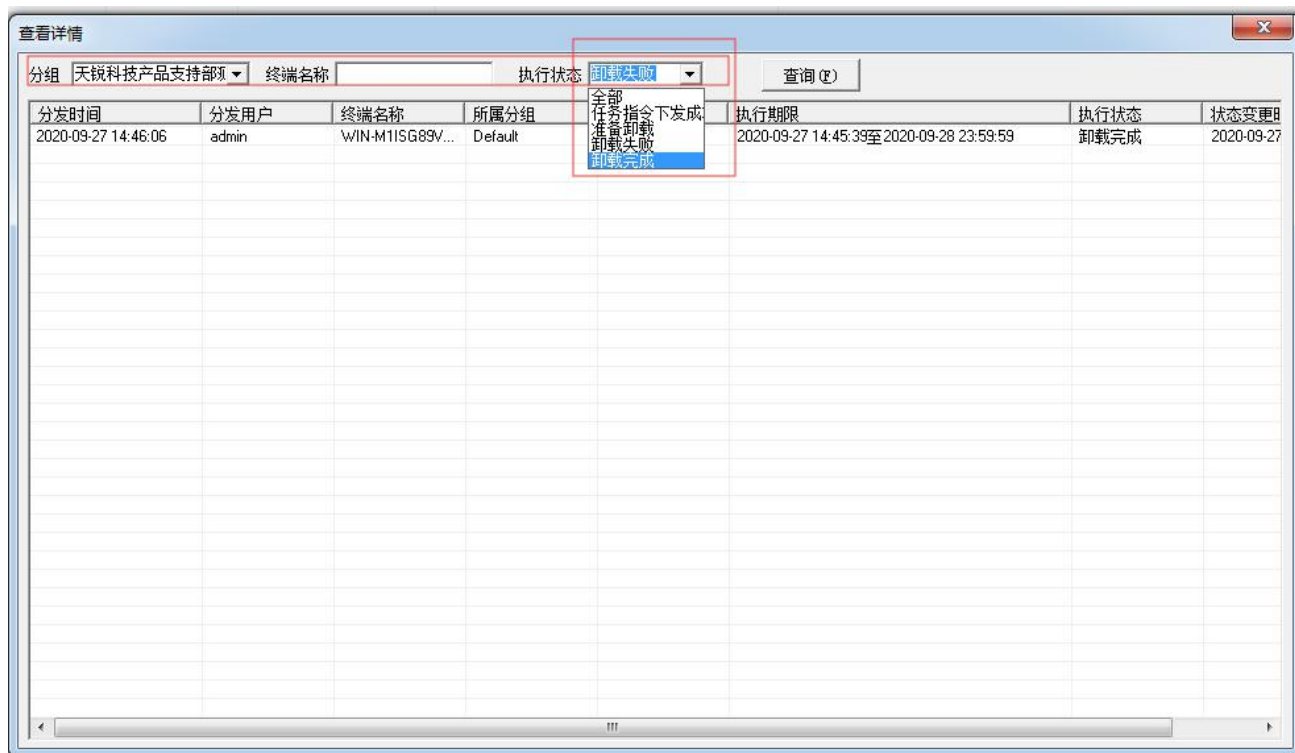


修改任务的执行有效期。在“任务分发情况”列表中，选择需要修改有效期的任务，鼠标右击选择“修改执行有效期”菜单，弹出“修改执行有效期”窗口，修改完成后，点击“确定”即可。如下图所示：



查看任务分发详情。在“任务分发情况”列表中，选择要查看详情的任务，鼠标右击选择

“查看详情”菜单，弹出“查看详情”窗口，可以根据分组、终端名称或执行状态来查询。如下图所示：



支持取消某个分发任务。在“任务分发情况”列表中，选择要取消的任务，鼠标右击选择“取消”按钮，列表将不再显示该任务。

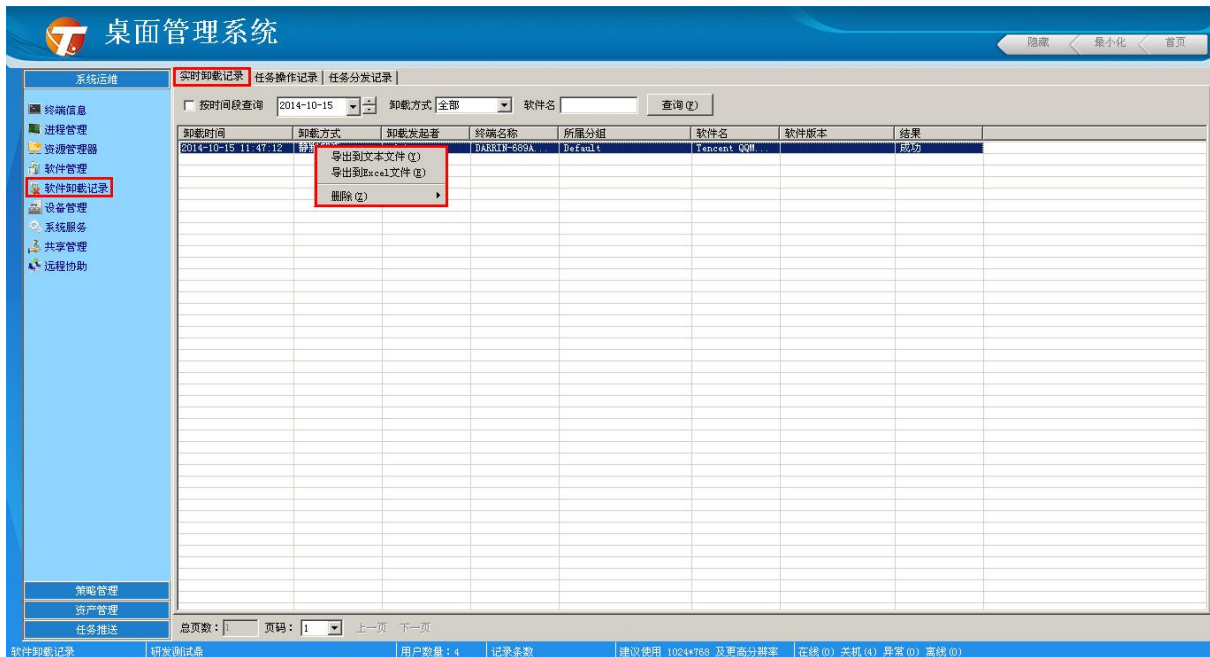
对已完成的分发任务可以设置完成。在“任务分发情况”列表中，选择要设置完成的分发任务，鼠标右击选择“确定”按钮，列表中不再显示该任务。

2.1.5 软件卸载记录

查看从控制台远程卸载终端电脑上软件的记录。包含有实时卸载记录、任务操作记录、任务分发记录。

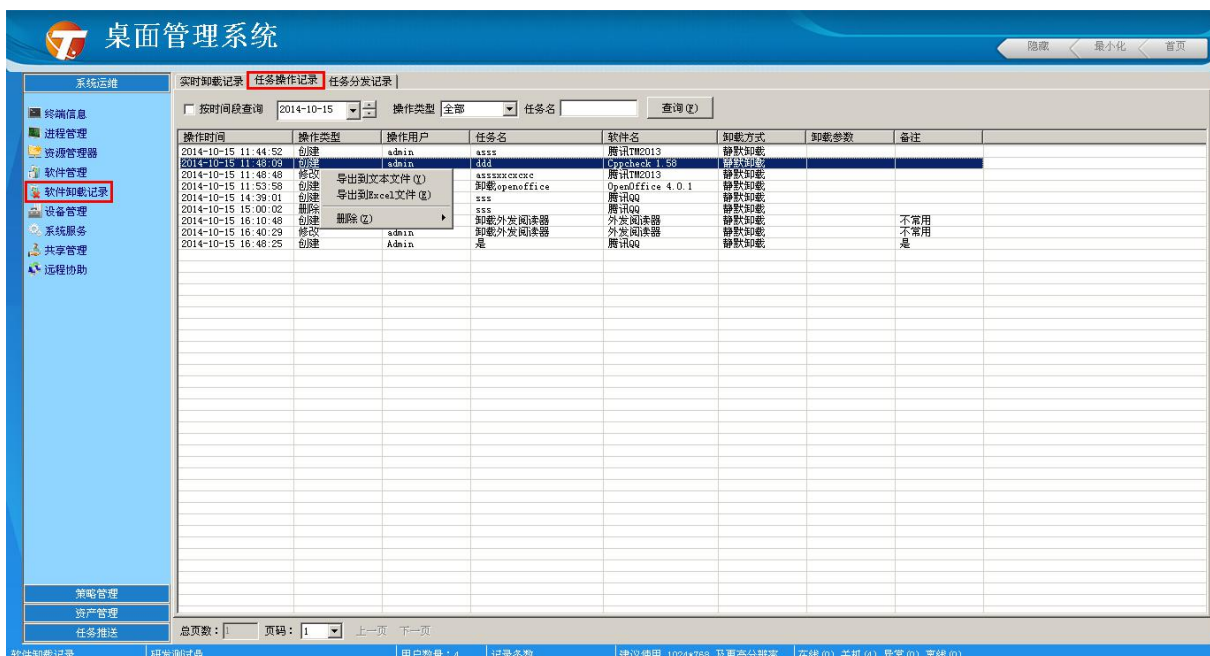
2.1.5.1 实时卸载记录

查看从控制台上直接远程卸载（非任务方式）终端电脑上软件的记录。在控制台的功能栏选择“系统运维”-“软件卸载记录”-“实时卸载记录”，支持导出或删除卸载记录。如下图所示：



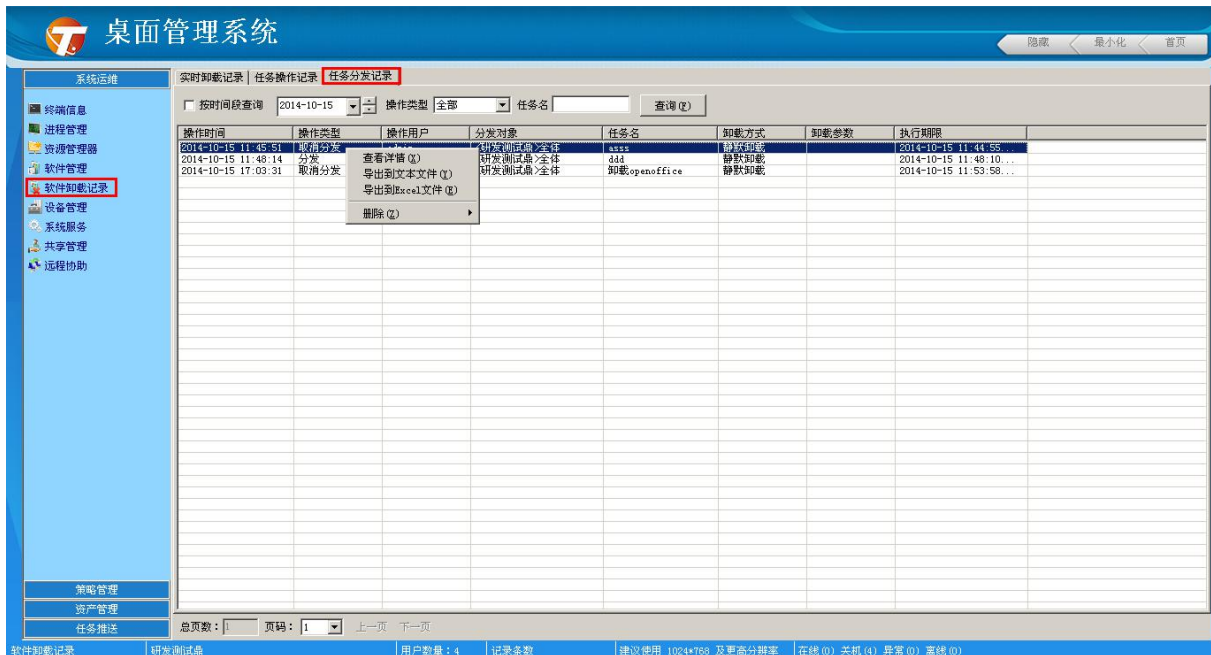
2.1.5.2 任务操作记录

查看任务的操作情况，记录管理员创建、修改、删除任务的记录。在控制台的功能栏选择“系统运维”-“软件卸载记录”-“任务操作记录”，支持导出或删除任务操作记录。如下图所示：

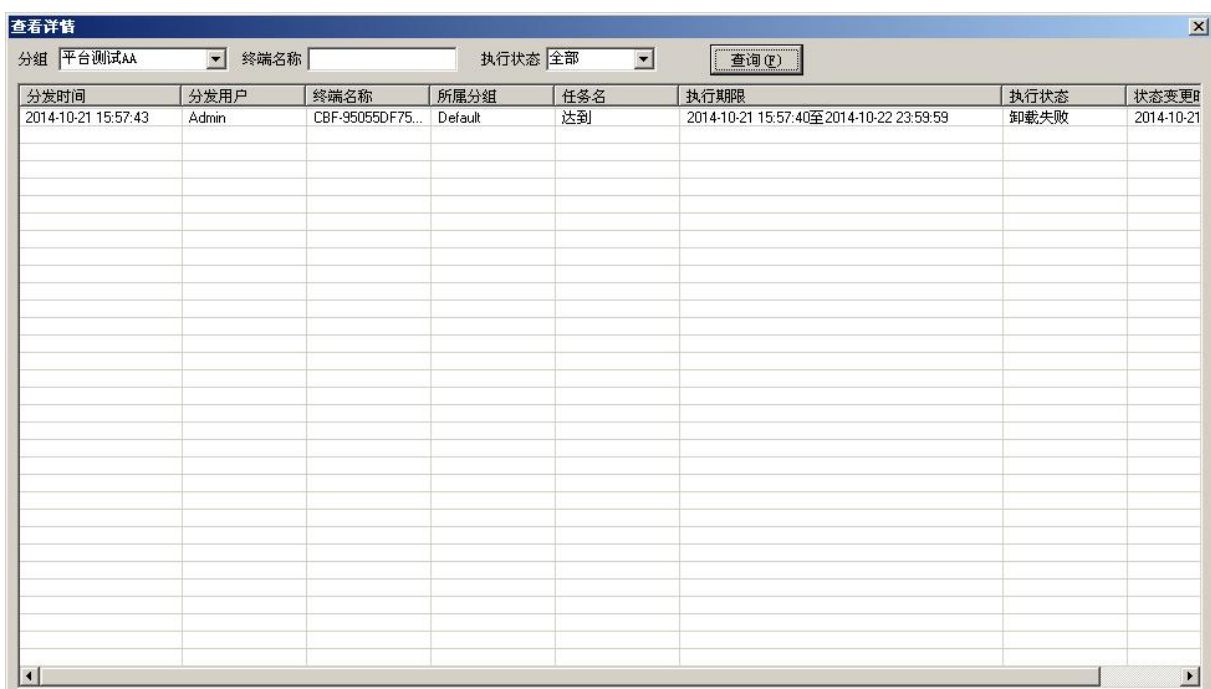


2.1.5.3任务分发记录

查看已完成分发或取消分发的任务记录。在控制台的功能栏选择“系统运维”-“软件卸载记录”-“任务分发记录”，对已完成分发的任务，可以查看任务执行详情。支持导出或删除任务分发记录。如下图所示：

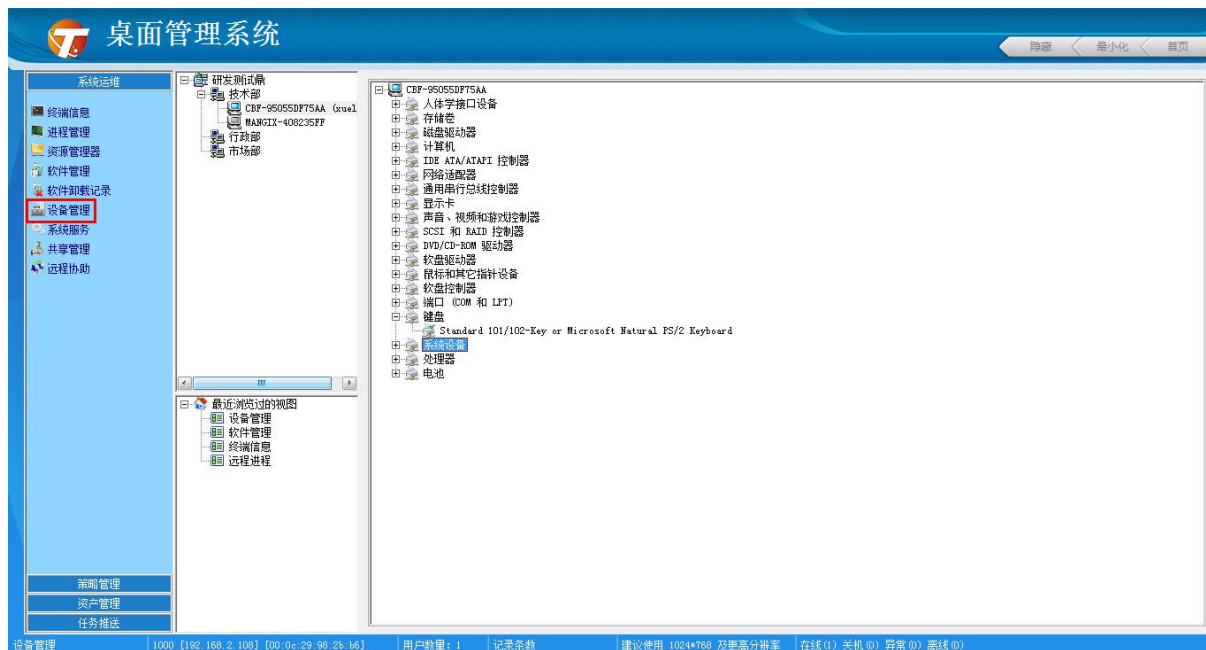


可以查看某任务分发的详情，包括任务分发时间、分发对象、执行状态、状态变更时间等。在任务分发记录列表中选择需要查看详情的任务，鼠标右击选择“查看详情”菜单，弹出“查看详情”窗口。如下图所示：



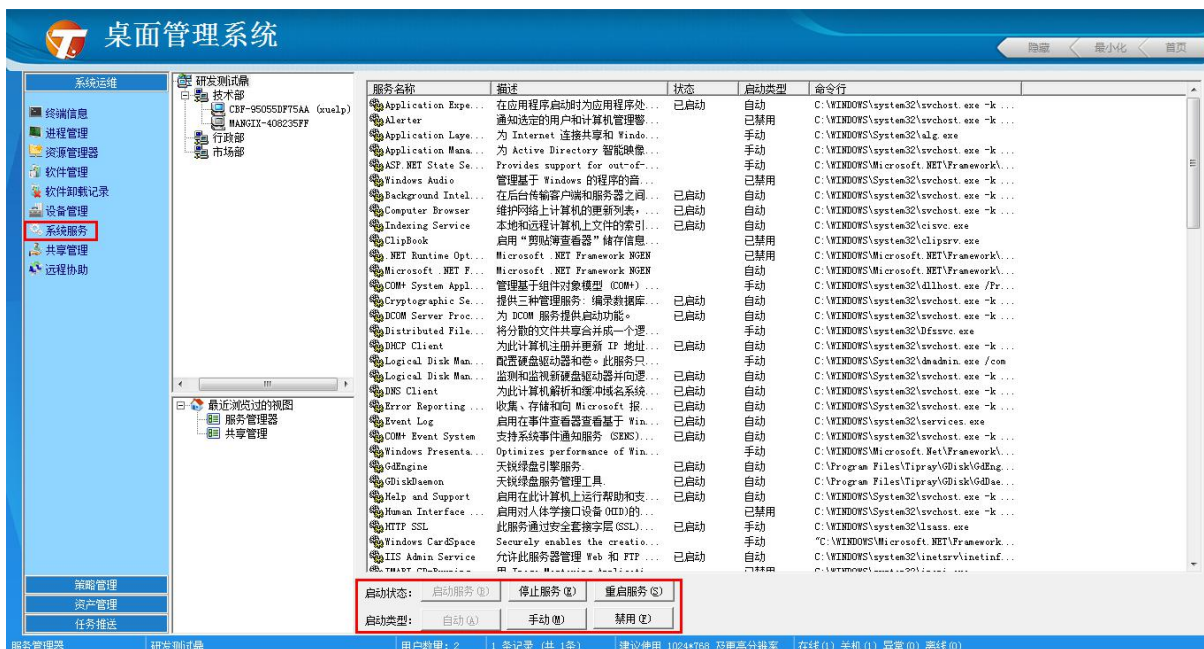
2.1.6 设备管理

在控制台的功能栏选择“系统运维”-“设备管理”，用户列表栏选择要查看的用户，详细信息栏将列出终端电脑上的设备信息。与终端电脑的设备管理器功能效果一样，可以禁用或启用某些设备的使用。如下图所示：



2.1.7 系统服务

在控制台的功能栏选择“系统运维”-“系统服务”，用户列表栏选择要查看的用户，详细信息栏将显示选中用户电脑当前运行的系统服务。选中某个服务，鼠标右键选择相应菜单，或单击详细信息栏底端的功能按钮，可以改变启动服务的状态（启动、停止和重启）和启动类型（自动、手动和禁用）。如下图所示：

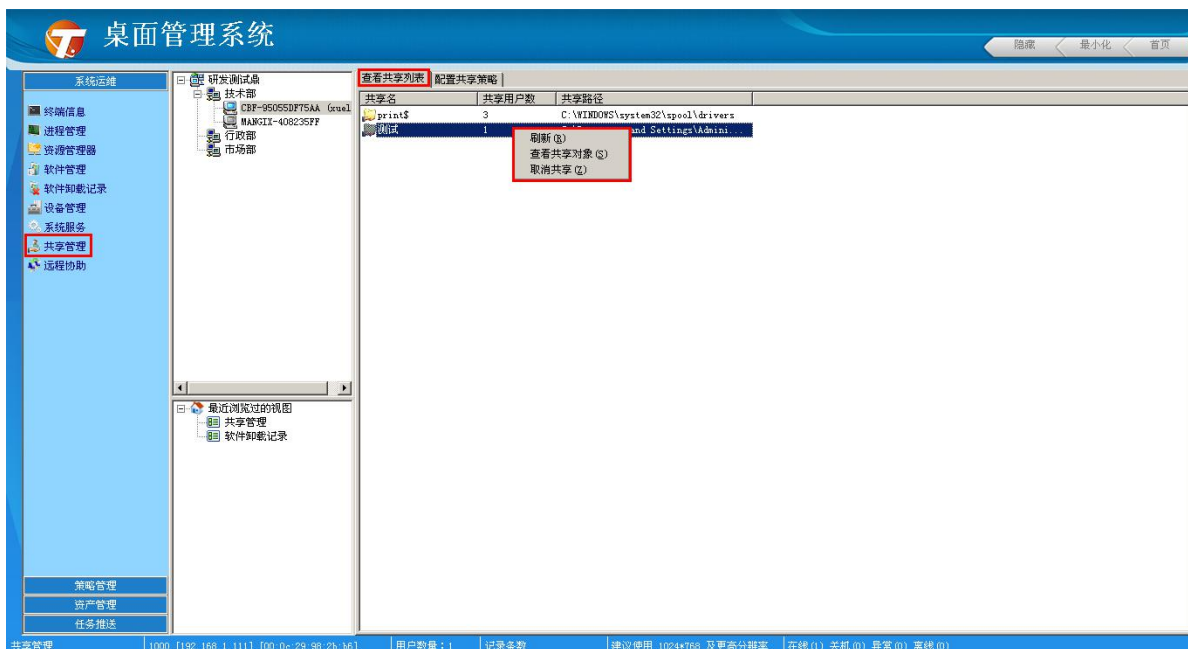


2.1.8 共享管理

查看终端电脑共享的文件夹及共享对象，可以根据需要取消共享或禁止共享服务。

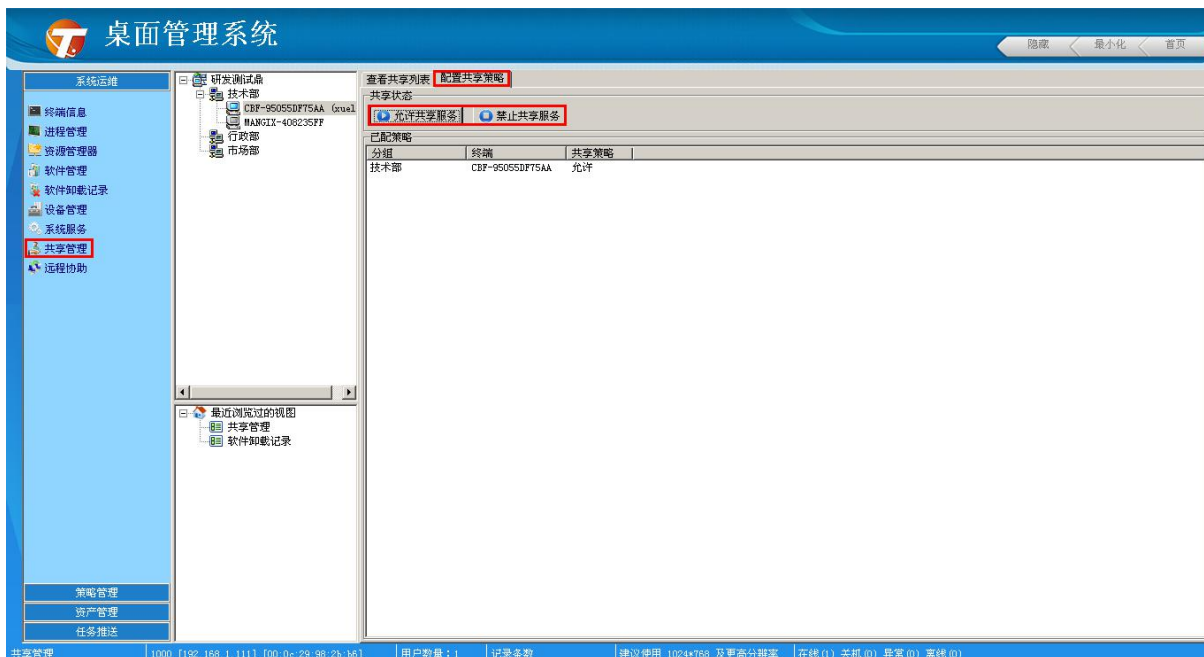
2.1.8.1 查看共享列表

在控制台的功能栏选择“系统运维”-“共享管理”-“查看共享列表”，用户列表栏选择要查看的用户，详细信息栏将显示该用户共享的文件目录列表。鼠标右击文件目录，可以查看共享对象或取消共享操作。如下图所示：



2.1.8.2 配置共享策略

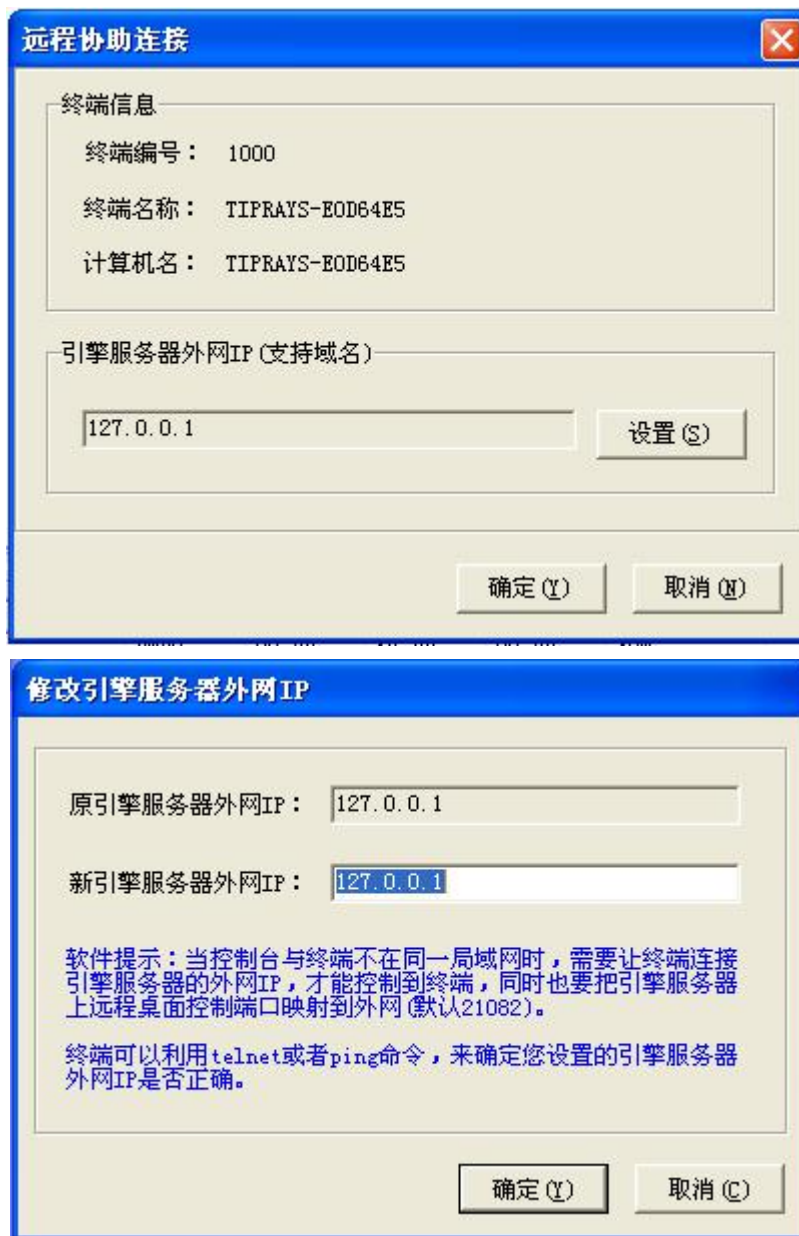
启动或关闭终端用户共享服务。点击“允许共享服务”按钮，则开启共享服务，点击“禁止共享服务”按钮，则关闭共享服务。如下图所示：



2.1.9 远程协助

在控制台用户列表栏选中要远程协助的终端，功能栏选择“系统运维”-“远程协助”，

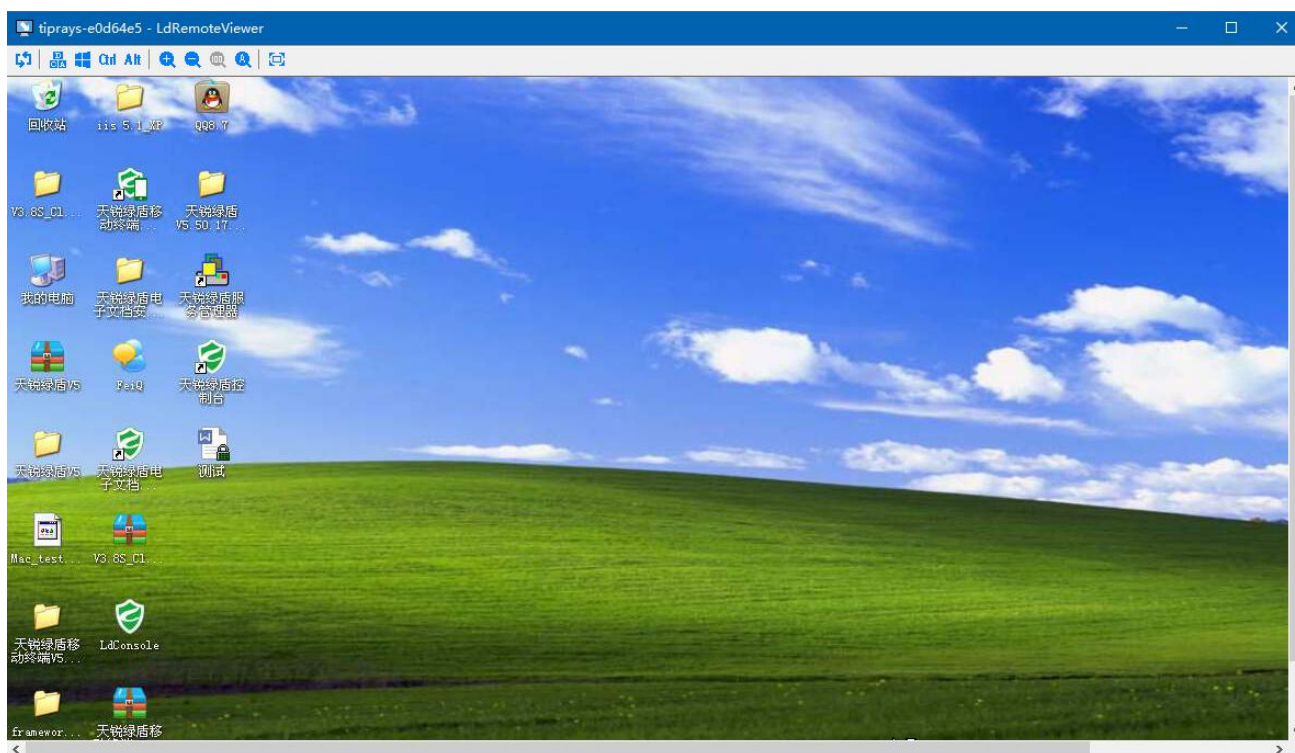
弹出“远程协助连接”窗口，需要设置引擎服务器 IP 地址，如果控制台和终端不在同一局域网内，则要让终端连接引擎服务器的外网 IP 才能控制到终端。同时也要把引擎服务器上远程桌面控制端口映射到外网（默认 21082）。如下图所示：



设置完成后，终端电脑上将弹出远程协助许可提示，可选择“接受”或“拒绝”，如果 26 秒内没有选择的话，将会自动拒绝被控制。如下图所示：



终端允许控制后，管理员即可在控制台上对终端电脑进行远程操作（另外还支持远程切换用户、锁屏和热键操作）。如下图所示：



2.1.10 远程控制

可以远程控制终端计算机，包括锁定、解锁、重启、注销、关闭计算机等，可以远程给终端发送消息。在用户列表中选中终端用户（可以选择公司名称、分组或终端），然后鼠标右键--远程控制，再选择相应的操作选项。如下图所示：



说明:此功能支持 Windows 和 Mac 终端。

2.2 策略管理

2.2.1 应用程序限制

限制终端电脑的应用程序使用，可以通过程序进程、窗口标题和软件版本限制三种方式进行限制。

2.2.1.1 程序限制

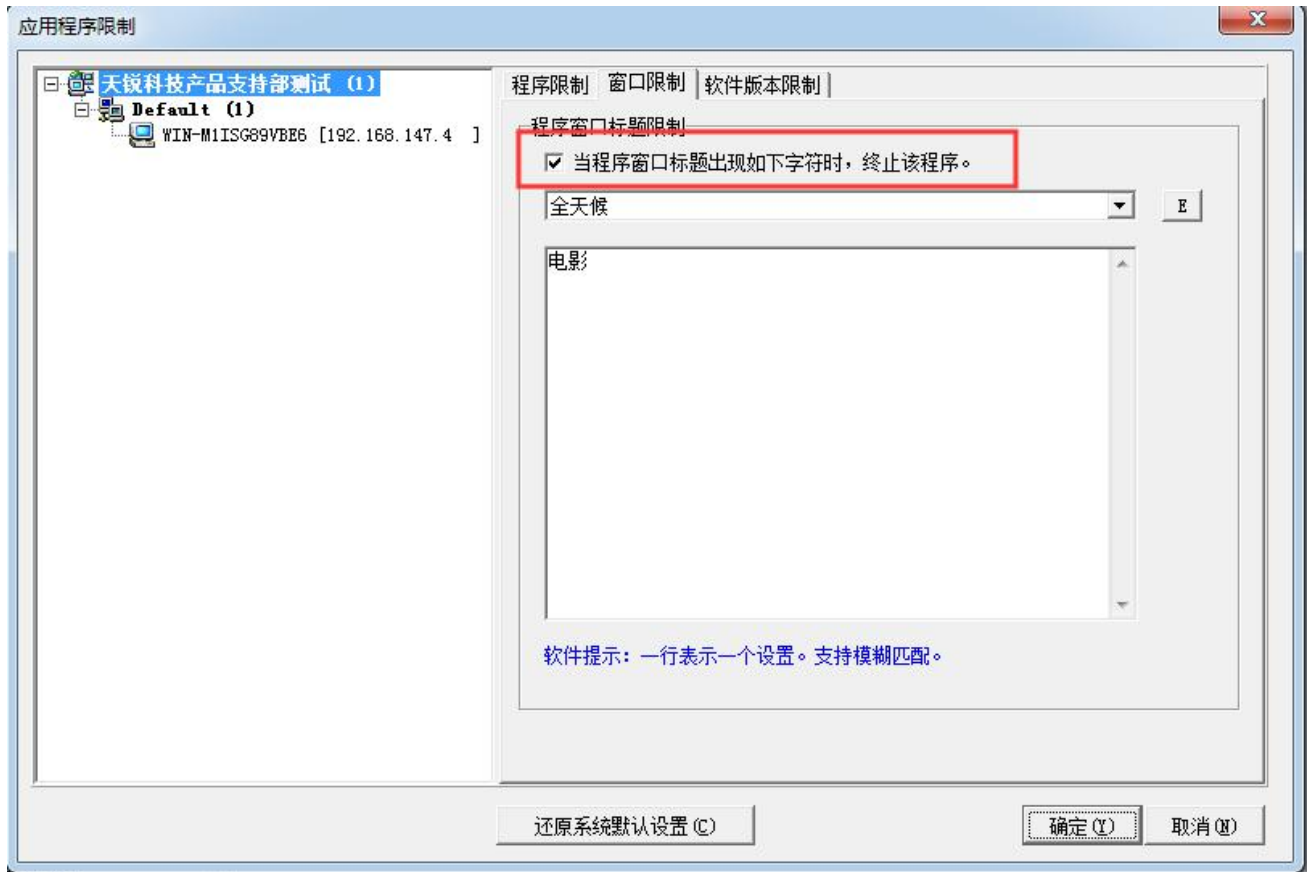
在控制台的功能栏选择“策略管理”-“应用程序限制”，在弹出的“应用程序限制”窗口左侧的用户列表选择要限制的用户（可以选择公司名称、分组或终端），在“程序限制”页面先选中禁止或只允许下列应用程序选项，再勾选相应的程序。系统内置了系统软件、办公软件、聊天工具、游戏娱乐等 9 类应用程序的部分程序。

支持自定义添加应用程序，添加方法如下：在需要添加的类别处右键鼠标，选择“添加应用程序”，在弹出的“添加应用程序”窗口中填写“程序描述”，点击“程序文件名”栏处的“E”按钮，找到要添加的应用程序的可执行程序，点击“确定”。可以新建程序类别，方法是鼠标右键“应用程序列表”根节点--添加应用程序类别。如下图所示：

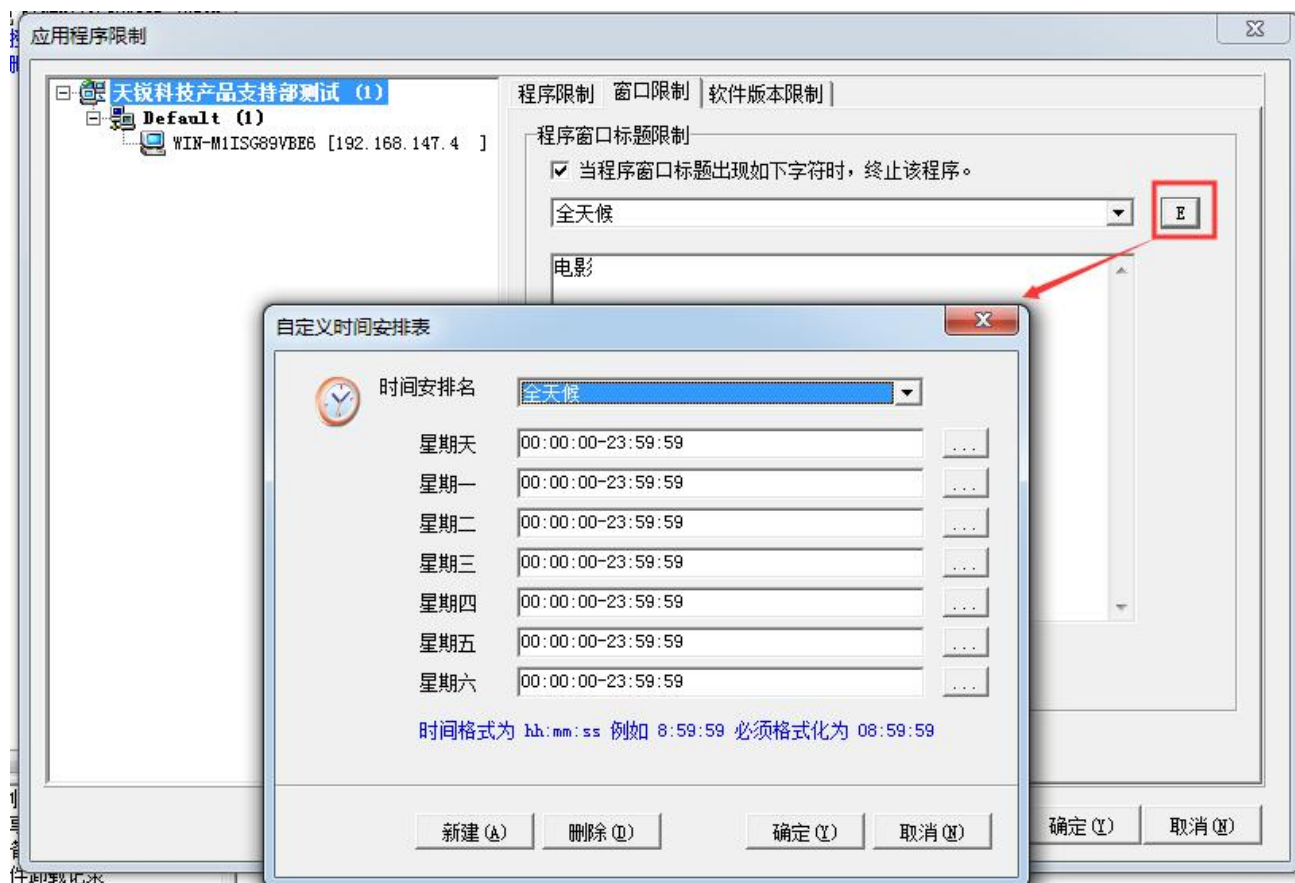


2.2.1.2 窗口限制

在“应用程序限制”窗口切换到“窗口限制”页面，在左侧的用户列表选择要限制的用户（可以选择公司名称、分组或终端），在窗口右侧勾选“当程序窗口标题出现如下字符时，终止该程序”选项，然后在文本框中输入要限制的窗口标题关键字，每行表示一个限制，设置完毕，点击“确定”。如下图所示：



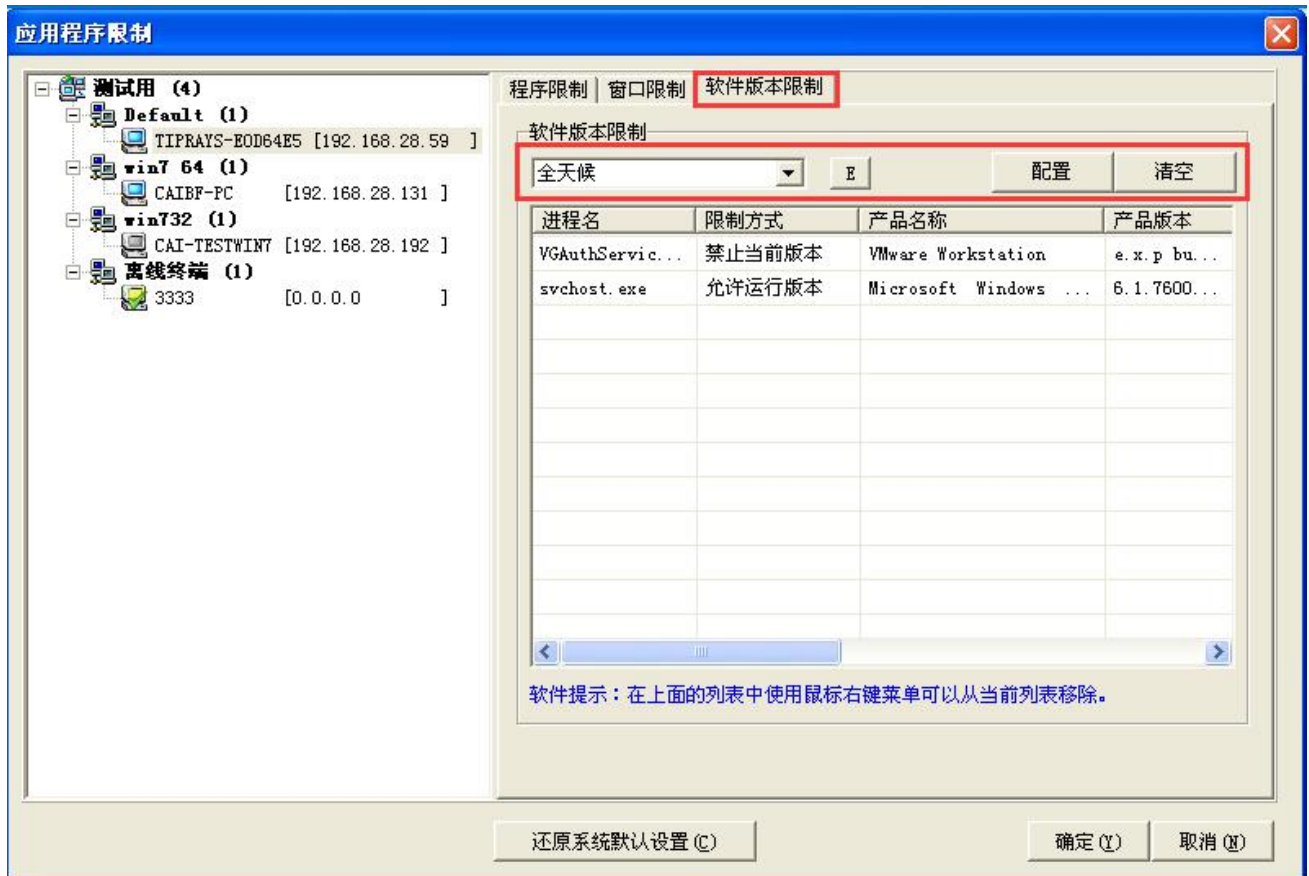
程序限制和窗口标题限制都可以设定时间规则，即在指定的时间段内限制生效。点击窗口中的“E”按钮进行时间定义。系统默认“全天候”时间安排表，可新建新的时间安排表或修改已有的时间安排表。如下图所示：



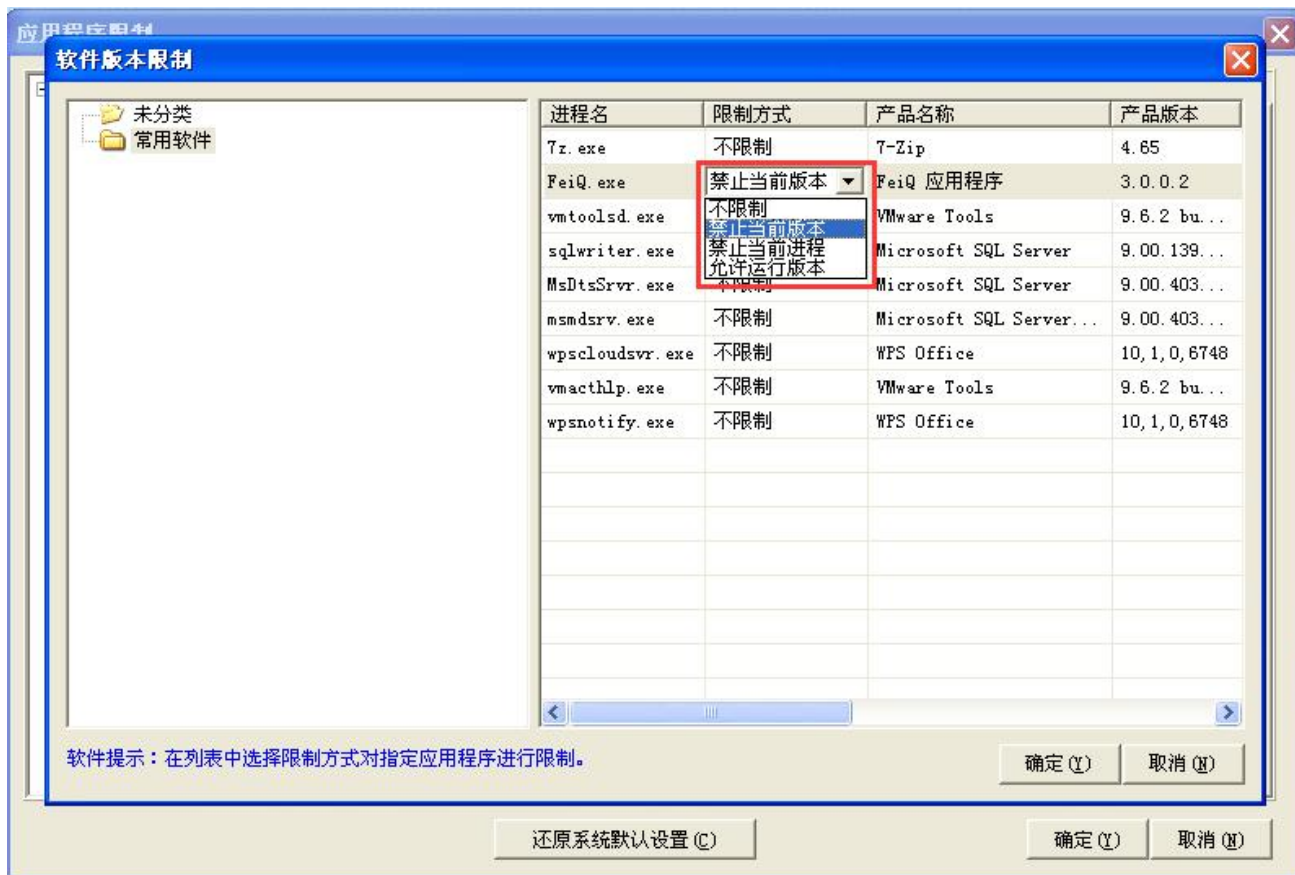
2.2.1.3 软件版本限制

对终端使用的软件版本可以根据需要设置允许或禁止使用当前版本，也可以禁止使用该进程。

在控制台的功能栏选择“策略管理”-“应用程序限制”，将弹出“应用程序限制”窗口。在左侧选择需要设置的对象（可以选择公司名称、分组或终端），在右侧选择“软件版本限制”进行配置策略，如下图所示：



点击“配置”，弹出“软件版本”限制窗口，在左侧选择需要配置的软件分组，在右侧软件版本列表中选择要配置的进程名以及产品版本，然后选择限制方式。配置完软件版本策略后，可以对指定策略设置时间限制，限制该策略在什么时间段生效。如下图所示：



四种限制方式：

不限制：不限制该进程对应的软件版本。

禁止当前版本：禁止使用该进程对应的软件版本。

禁止当前进程：禁止同进程名的软件。

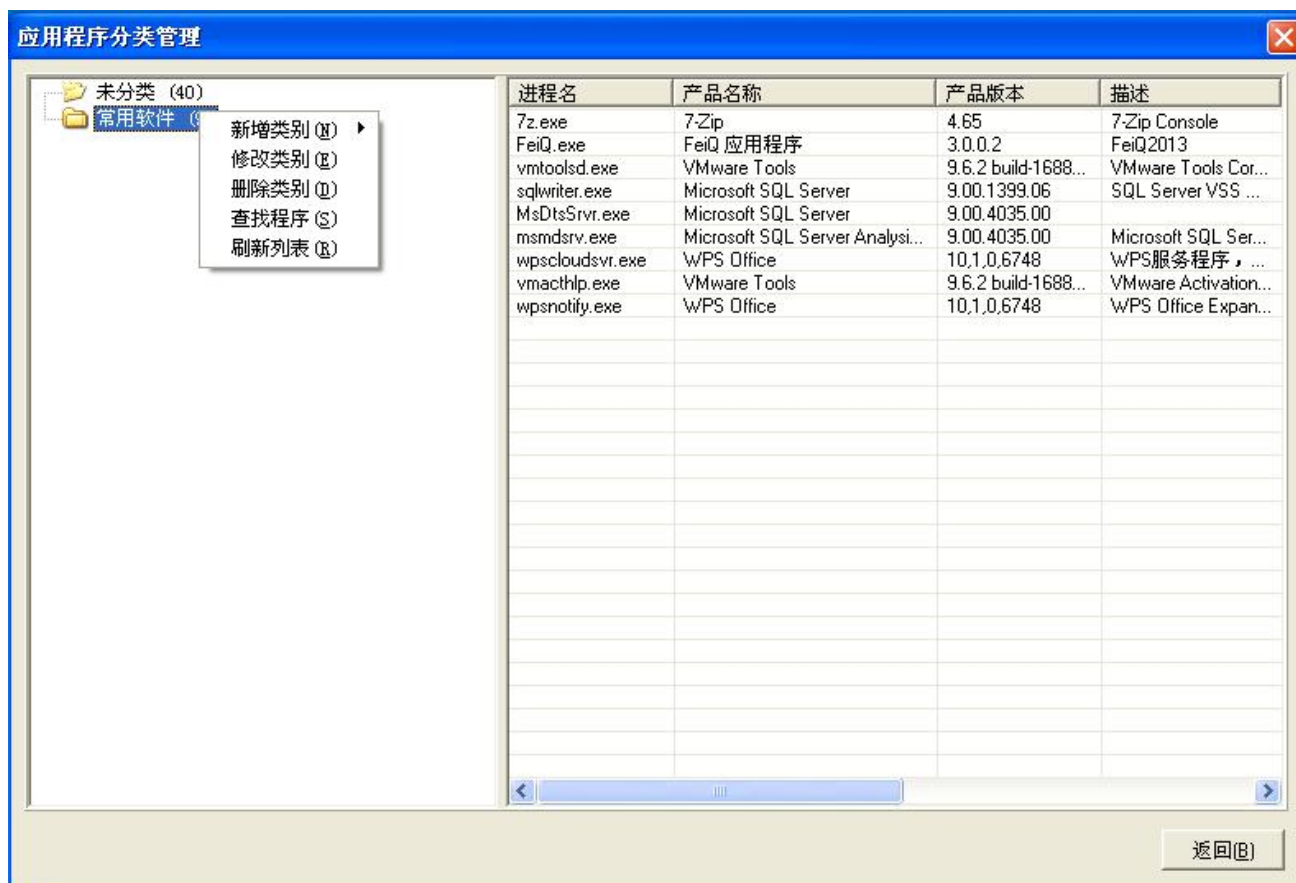
允许运行版本：禁止同进程名的软件，但允许例外版本的软件。

说明：窗口左侧的软件分组设置可以到“策略管理”-“应用程序分类管理”进行设置。

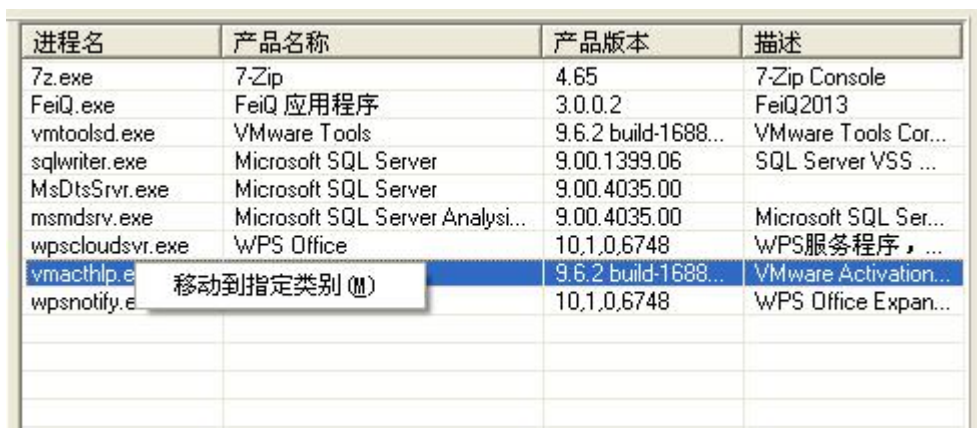
2.2.2 应用程序分类管理

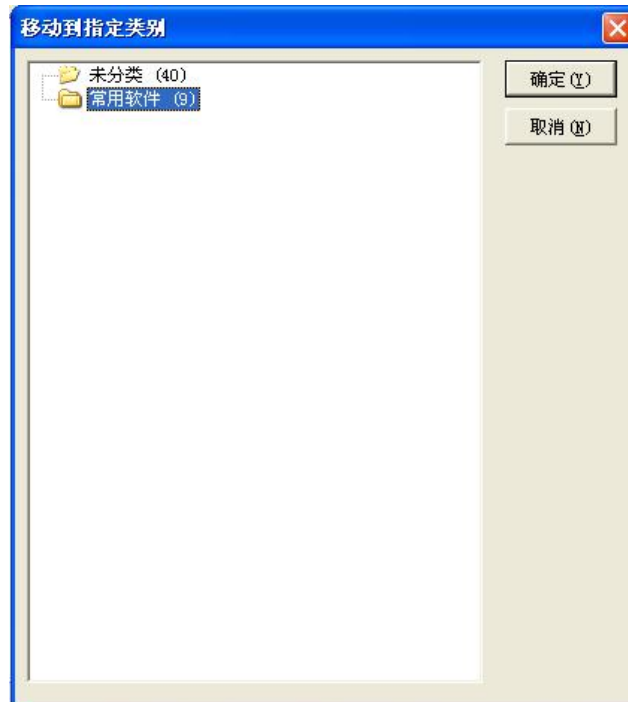
采集终端上使用的软件信息，并根据需要对软件进行分类管理。

在控制台的功能栏选择“策略管理”-“应用程序分类管理”，将弹出“应用程序分类”窗口，在左侧右键点击支持增删改软件类别操作，还支持查找程序和刷新列表，如下图所示：



在右侧可以选择要移动类别的对象，然后鼠标右键点击“移动到指定类别”，弹出窗口，选择要移动的分类，点击确定即可。如下图所示：



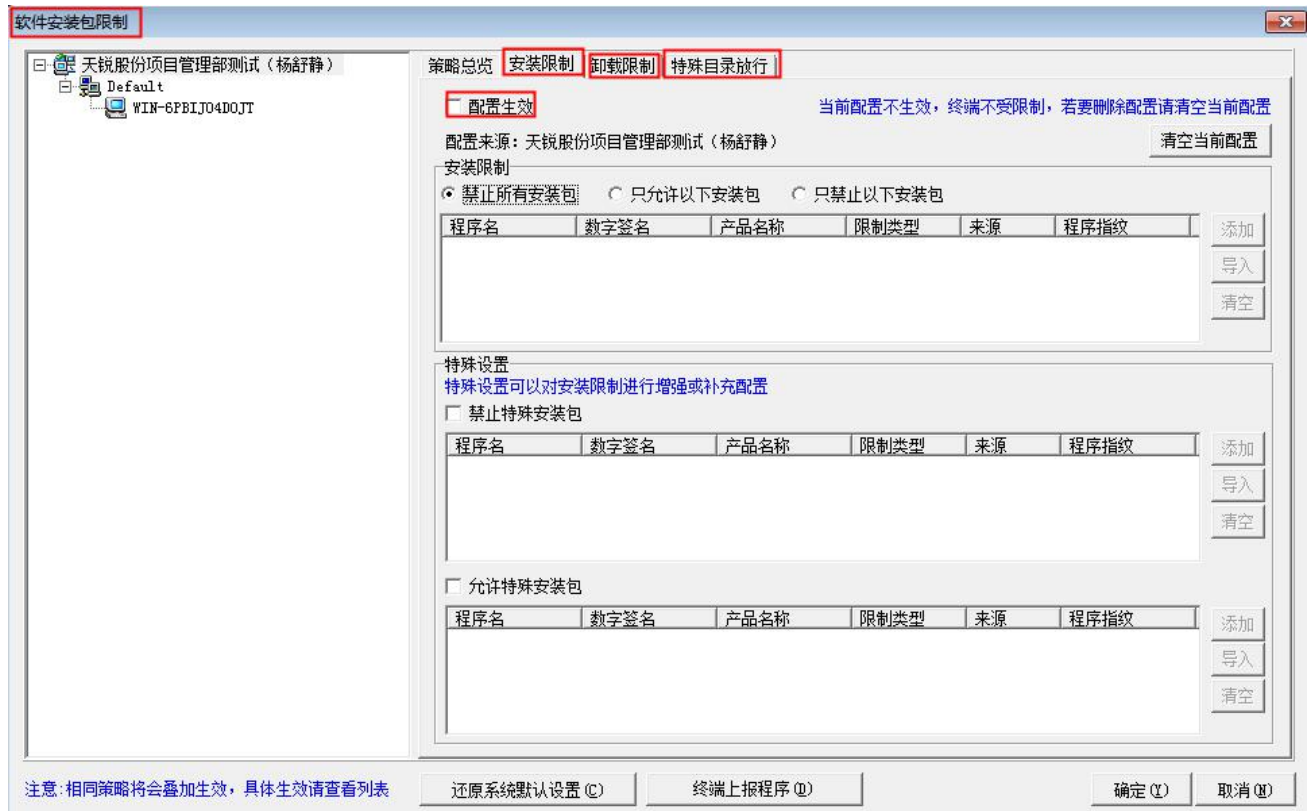


2.2.3 软件安装包限制

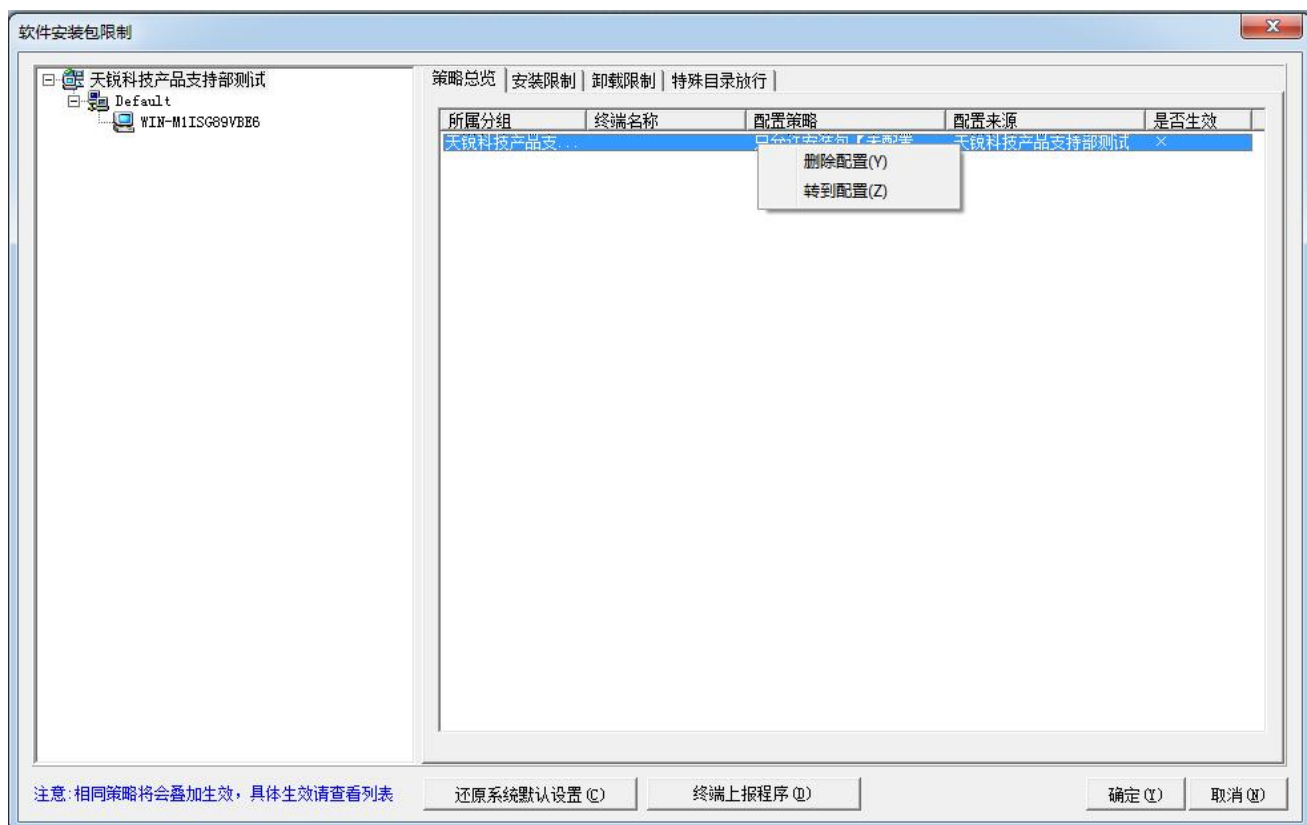
根据软件程序指纹、产品名称、数字签名等限制指定终端禁止、只允许安装指定软件。

在控制台的功能栏“策略管理”-“软件安装包限制”，将弹出“软件安装包限制”窗口。

在左侧选择需要设置的对象（可以选择分组或终端），在右侧选择“安装限制”页，设置安装策略并勾选“配置生效”点击“确定”即生效。当需要添加多个软件时，点击“添加”即弹出“添加程序”窗口，选择“批量添加”点击“选择目录”选择需要添加的程序，并勾选点击“确定”即可批量添加程序。

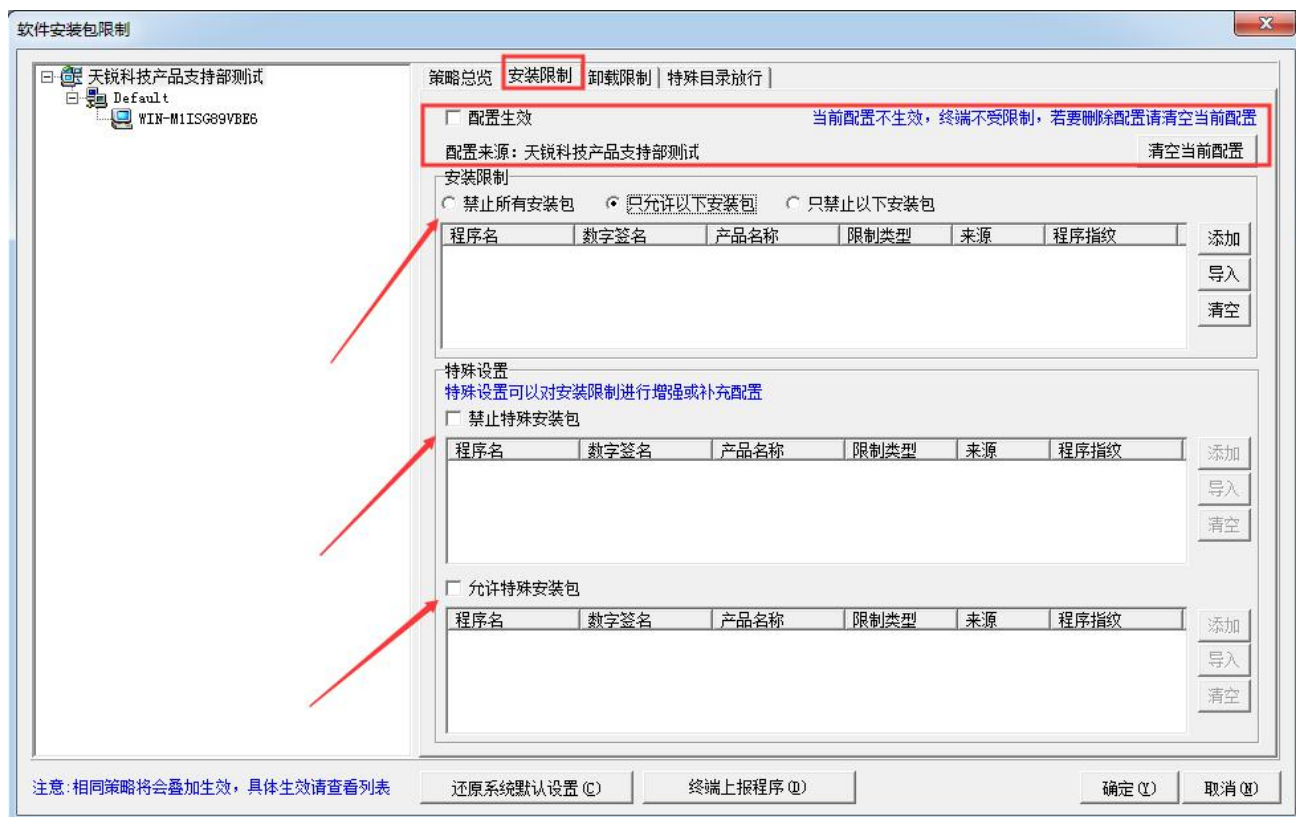


2.2.3.1 策略总览



点击桌面管理系统-策略管理-策略总览，可以查看整个的软件安装包限制配置。对应选择配置，右键可以删除配置或者转到配置内容，具体查看详细配置信息。

2.2.3.2 安装限制



配置生效：勾选此项则会开启对应配置。

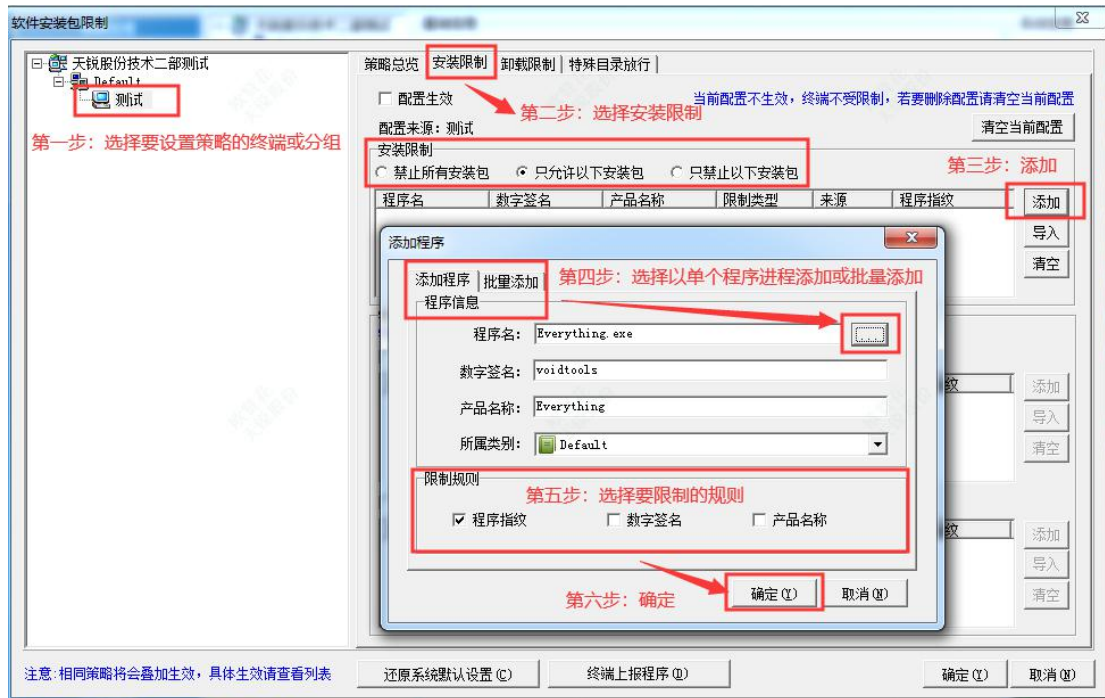
禁止所有安装包：勾选此项，则会限制所有软件安装包的安装；可以在下方的“允许特殊安装包”中“添加”或从软件库“导入”的方式添加程序设置软件安装包，此处设置的安装包则允许安装；

只允许以下安装包：勾选此项，则只允许部分软件安装包的安装；点击“添加”或软件库“导入”方式添加软件程序设置允许安装的安装包。

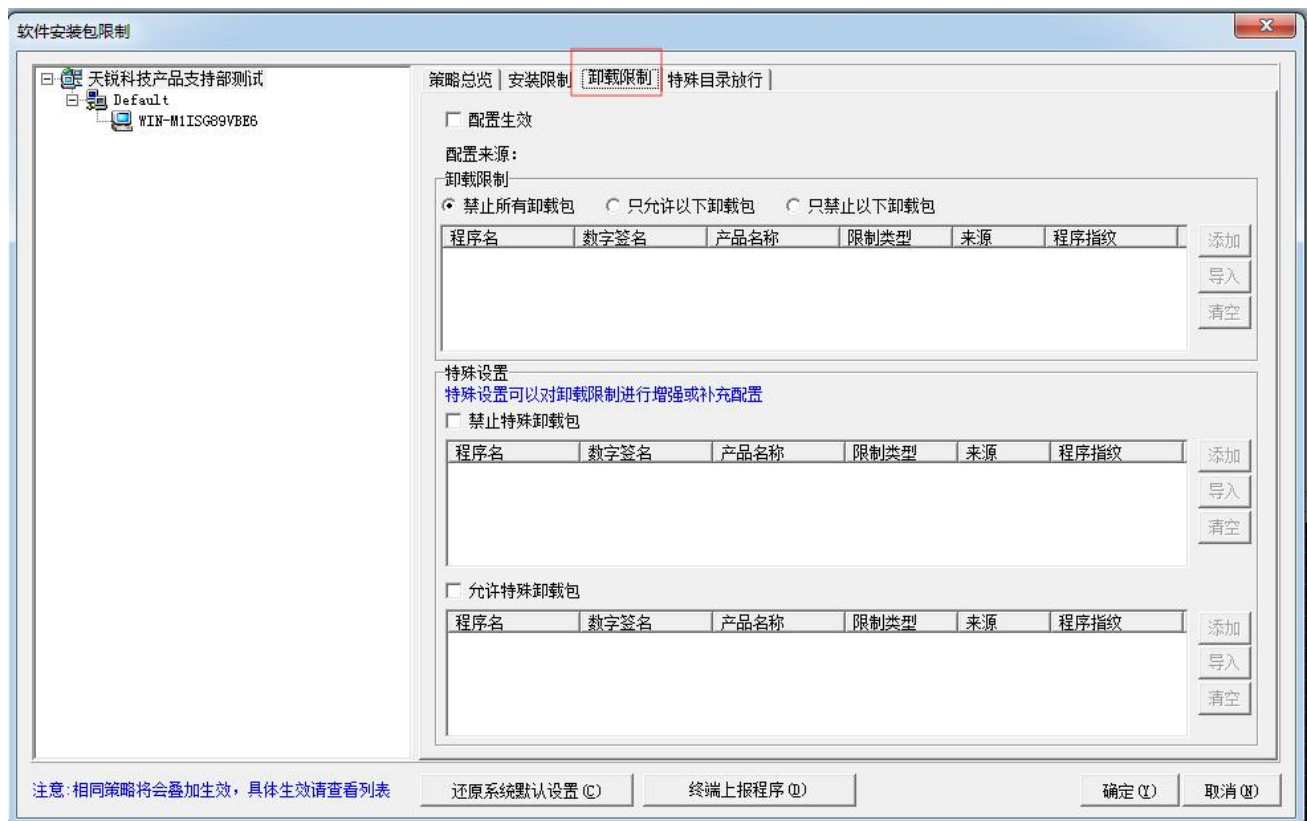
只禁止以下安装包：勾选此项，则只限制部分软件安装包的安装；点击“添加”或软件库“导入”方式添加软件程序设置禁止安装的安装包。

禁止特殊安装包：勾选此项，可以禁止配置里面的特殊安装包；点击“添加”或软件库“导入”方式添加软件

允许特殊安装包：勾选此项，可以允许配置里面的特殊安装包；点击“添加”或软件库“导入”方式添加软件



2.2.3.3 卸载限制



配置生效: 勾选此项则会开启对应配置

禁止所有卸载包:勾选此项,则会限制所有软件安装包的卸载;可以在下方的“允许特殊卸载包”中“添加”或从软件库“导入”的方式添加程序设置软件安装包,此处设置的安装包则允许卸载;

只允许以下卸载包:勾选此项,则只允许部分软件安装包的卸载;点击“添加”或软件库“导入”方式添加软件程序设置允许卸载的安装包。

只禁止以下卸载包:勾选此项,则只限制部分软件安装包的卸载;点击“添加”或软件库“导入”方式添加软件程序设置禁止卸载的安装包。

禁止特殊卸载包:勾选此项,可以禁止配置里面的特殊安装包;点击“添加”或软件库“导入”方式添加软件

允许特殊卸载包:勾选此项,可以允许配置里面的特殊安装包;点击“添加”或软件库“导入”方式添加软件



2.2.3.4特殊目录放行

在设定的特殊目录下的程序,执行安装(卸载)程序时,不受安装(卸载)限制。选择“特殊目录放行”,点击“添加”,输入要设置的放行的目录名,点击“确定”

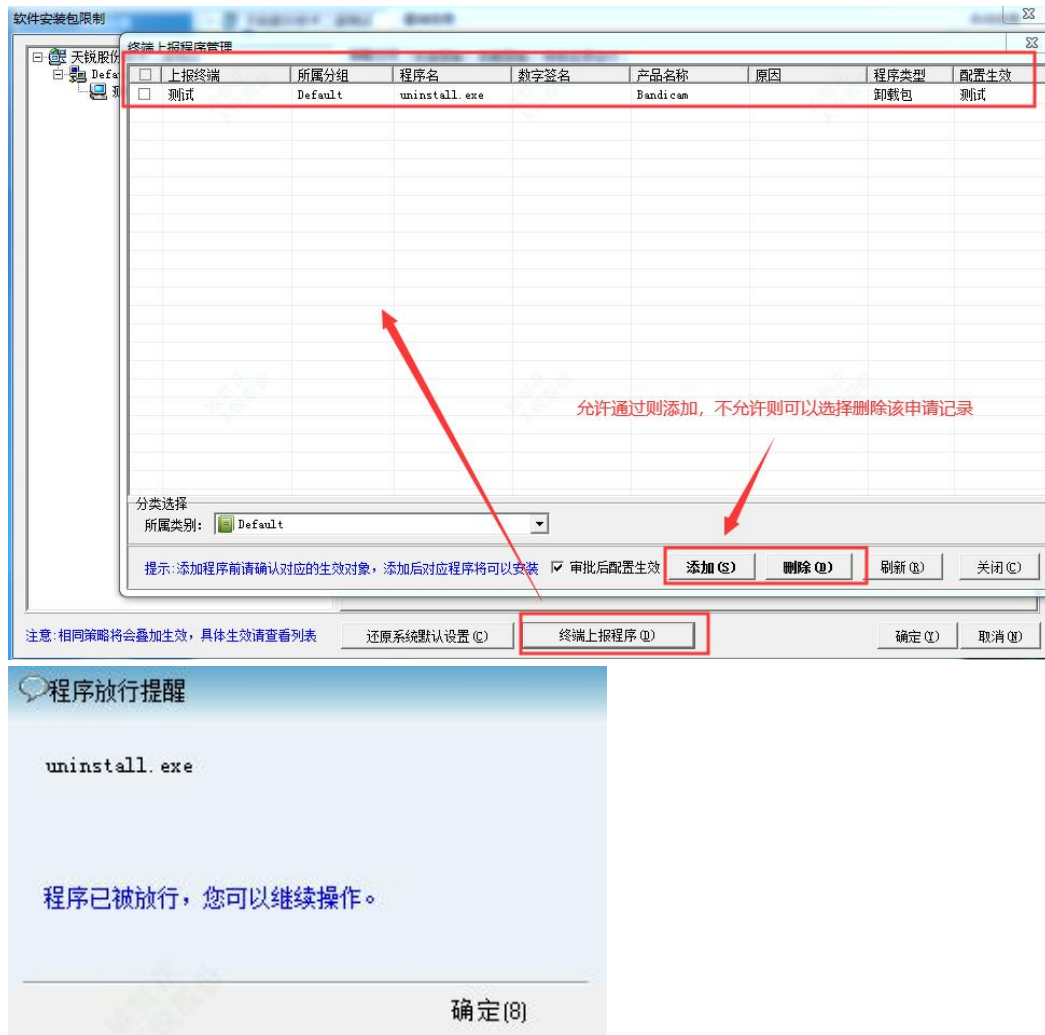


The screenshot shows a Windows XP desktop with a blue taskbar. In the background, there's a window titled "组织 卸载/更改" (Organization Uninstall/Change) displaying a list of installed programs. The list includes "360安全浏览器" (360 Safe Browser), "Bandicam" (highlighted with a red box), "Bandisoft MPEG-1 Decoder", and several instances of "Microsoft Corporation".

In the foreground, a "软件策略限制" (Software Restriction Policy Limitation) dialog box is open. It contains the message: "软件已被限制，如有疑问，请联系管理员。" (The software has been restricted. If you have any questions, please contact the administrator.) Below the message is a "确定" (OK) button.

A red arrow points from the "确定" button to the bottom right corner of the screen, where another dialog box titled "程序拦截提醒" (Program Interception Reminder) is visible. This dialog box displays the file path: "C:\Program Files (x86)\Bandicam\uninstall.exe". At the bottom of this dialog, there are two buttons: "上报程序" (Report Program) and "取消(9)" (Cancel(9)). The "上报程序" button is highlighted with a red box.

Below the "程序拦截提醒" dialog, there is a text overlay in Chinese: "当前运行的程序被拦截了，如果您希望继续执行该程序，请点击下方上报程序进行上报，等待管理员通过后再执行安装操作。" (The currently running program has been intercepted. If you want to continue executing the program, click the report program button below to report it, wait for the administrator's approval, and then perform the installation operation.)

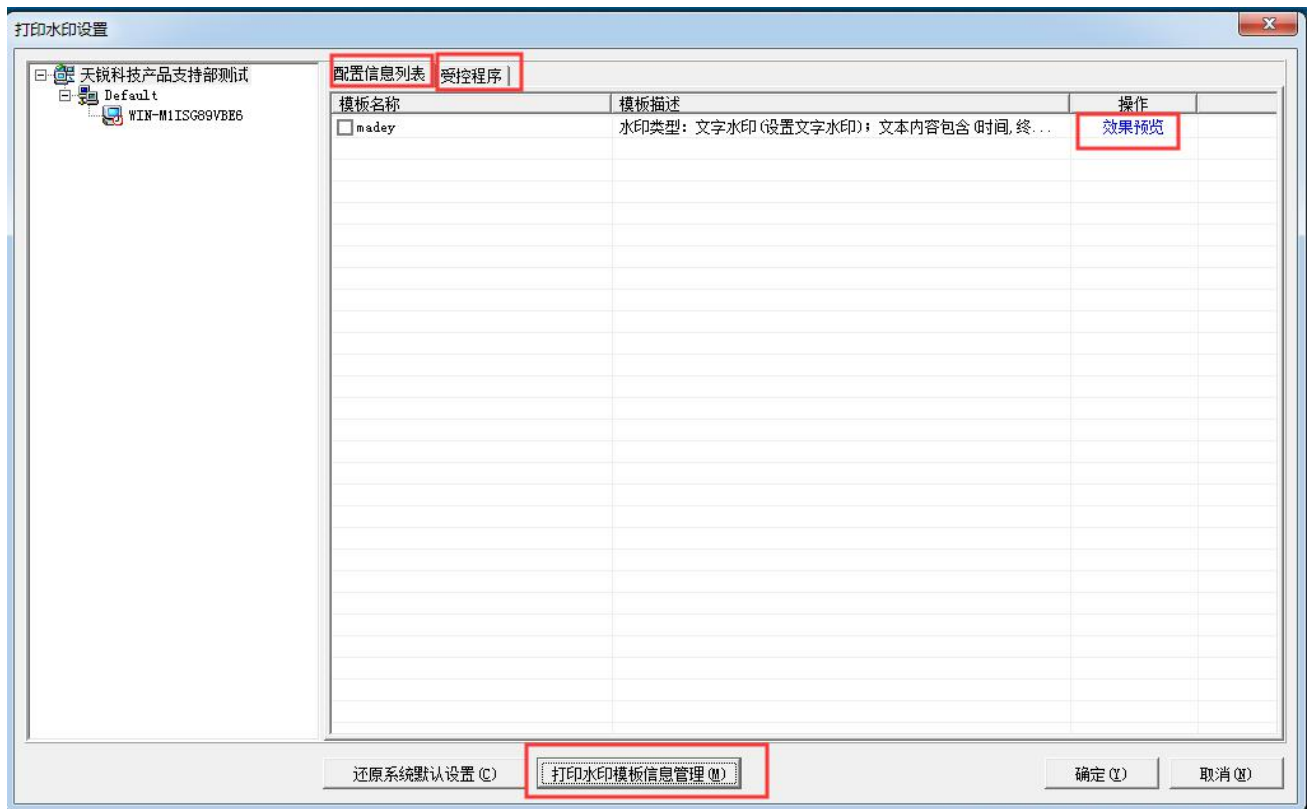


2.2.4 打印水印设置

2.2.4.1 配置信息列表

设置打印水印内容，用户可自行选择打印时是否需要水印。

在控制台的功能栏选择“策略管理”-“打印水印设置”，将弹出“打印水印设置”窗口。在左侧选择需要设置的对象（可以选择公司名称、分组或终端），在右侧可以预览水印效果，受控程序，并选择要设置的水印模板。如下图所示：



可以点击“打印水印模板信息管理”进行增删改水印操作。

勾选“设置文字参数”可以设置相应的文字水印内容。纯文本水印内容包括打印时间、操作员名称及自设内容。还可以对水印内容的字体类型、大小、颜色、形式、位置、形式（包含文字水印、二维码水印、点阵水印）进行设置，并可以根据需要自定义图层前景或背景显示。如下图所示：





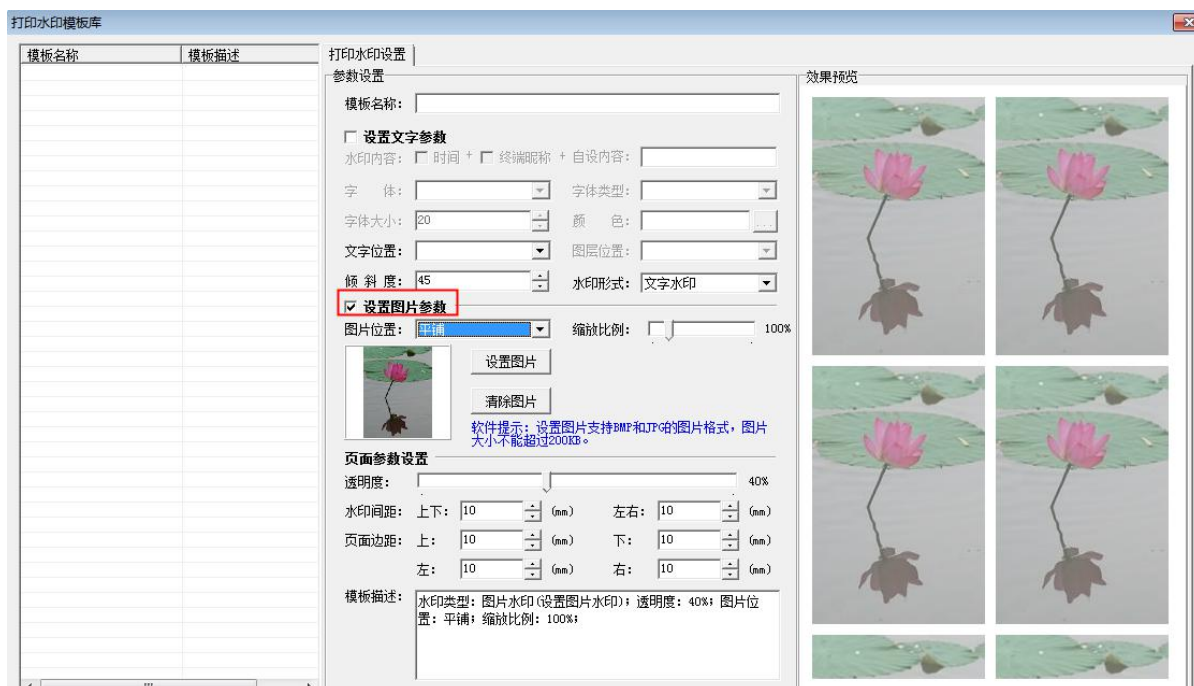
“文字水印”在打印内容界面上显现计算机相应的信息，水印信息包括自定义信息和操作者信息（终端昵称、时间、IP 地址和 MAC 地址等），管理员直接查看文件或者照片能知道是从哪台计算机上泄露出去的。

“二维码水印”二维码水印是通过二维码的形式展现水印。二维码水印在文件上进行展示。当资料

被外传通过扫描二维码可得到泄密信息的来源的相关信息。

“点阵水印”点阵水印是打印内容界面覆盖上一层包含自定义水印内容（包含时间、终端昵称、操作员名称、IP 地址、MAC 地址）的圆点图案。当机密信息被外传时，管理员在获取点阵水印图案后，可以通过控制台的【查询点阵码】得到泄密信息来源的相关信息（包括计算机名称、用户名称、IP、时间等），防止屏幕信息被泄露后出现无据可查的现象。

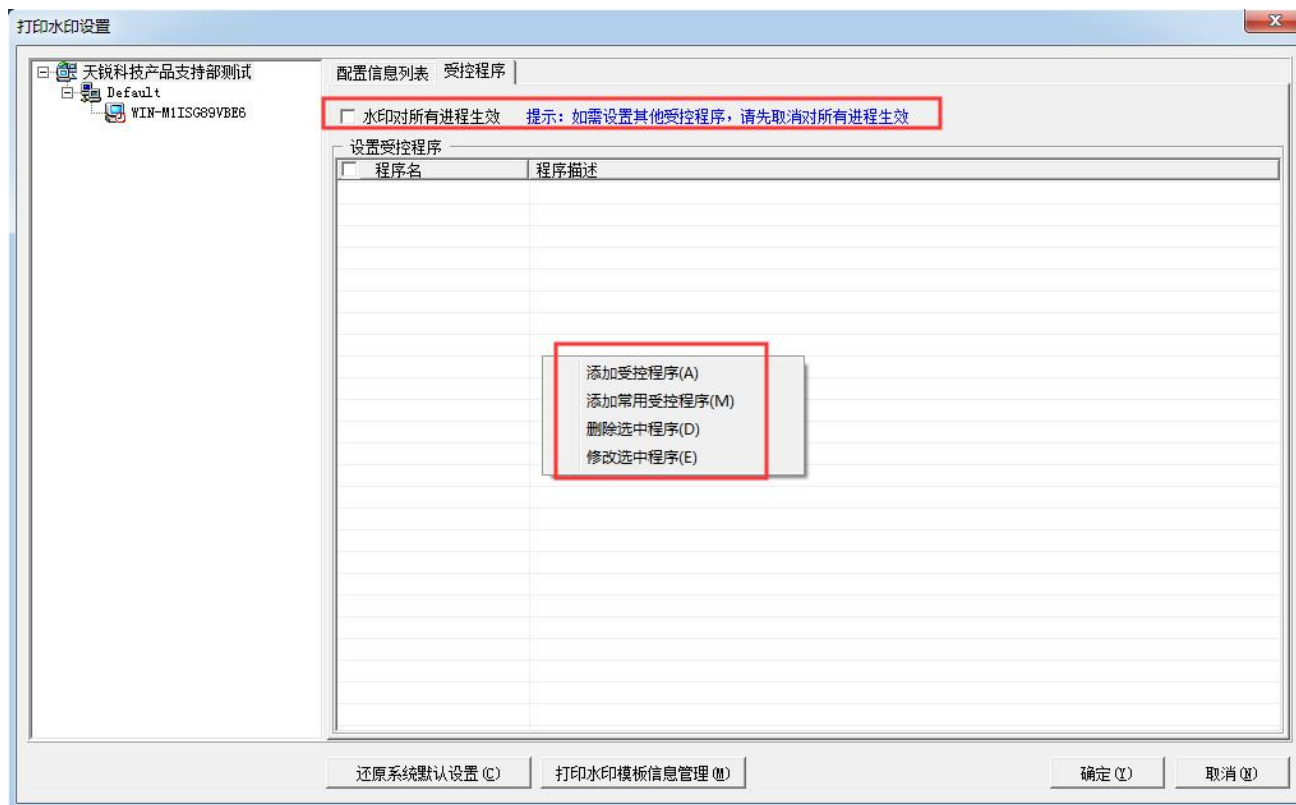
勾选“设置图片参数”可以设置相应的图片水印内容。图片水印内容包括设置图片和页面参数设置。其中页面参数设置包括图片的透明度、水印数量、水印间距和页面边距的设置。如下图所示：



2.2.4.2 受控程序

水印对所有进程生效：勾选此选项，所有的进程只要操作打印，都会对应有水印。

如果想要单独对应的程序，那么需要取消勾选“水印对所有进程生效”，在空白处，右键可以选择添加受控程序、添加常用受控程序（从库里面添加），删除选中程序或者修改选中程序然后进行勾选。如下图所示

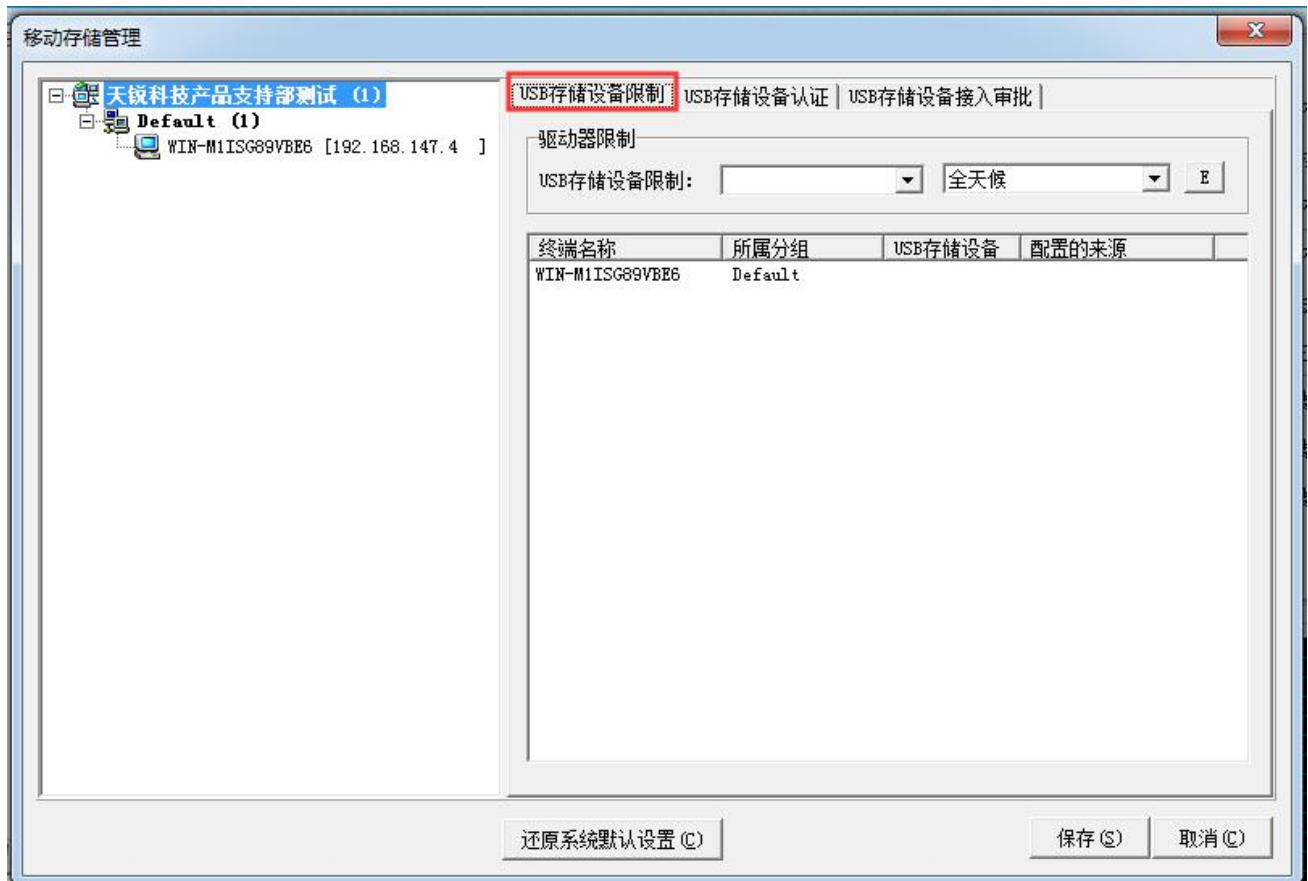


2.2.5 移动存储管理

USB 存储设置控制包括 USB 存储设备限制、USB 存储设备认证和 USB 存储设备接入审批三个功能，同时支持 Windows 终端和 Mac 终端，其中 USB 存储设备接入审批只支持 windows。

2.2.5.1 USB 存储设备限制

USB 存储设备限制可以设置终端全部允许使用（选择空白选项）、允许使用、禁止使用、只读 USB 存储设备和断网使用（即插入 USB 存储设备时终端断网），并可以设置限制在指定的时间段内生效。在控制台的功能栏选择“策略管理”-“移动存储管理”，在弹出的“USB 存储设备限制”窗口左侧选择需要限制的对象（可以选择公司名称、分组或终端），右边根据提示设置具体限制内容，设置完毕点击“保存”即可。如下图所示：

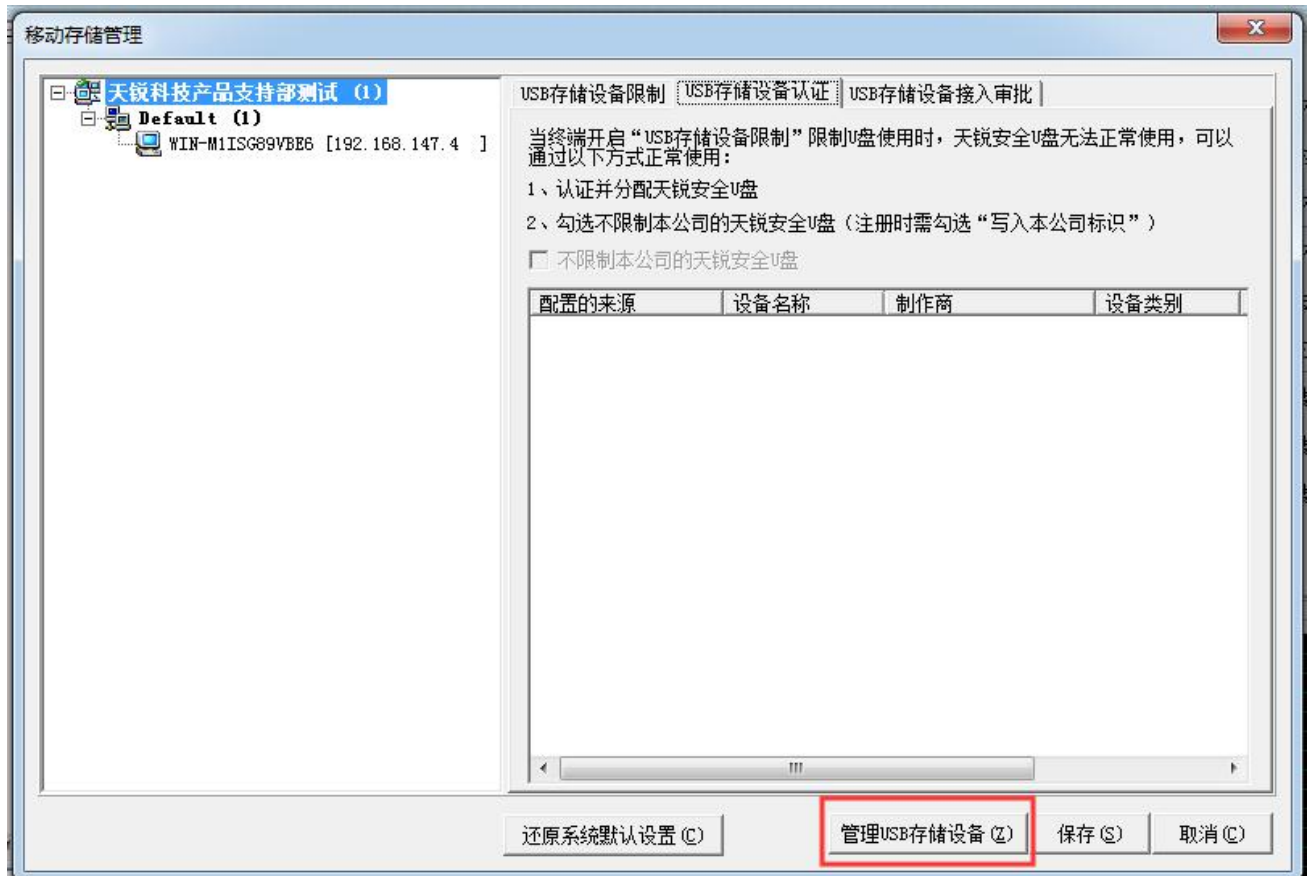


2.2.5.2 USB 存储设备认证

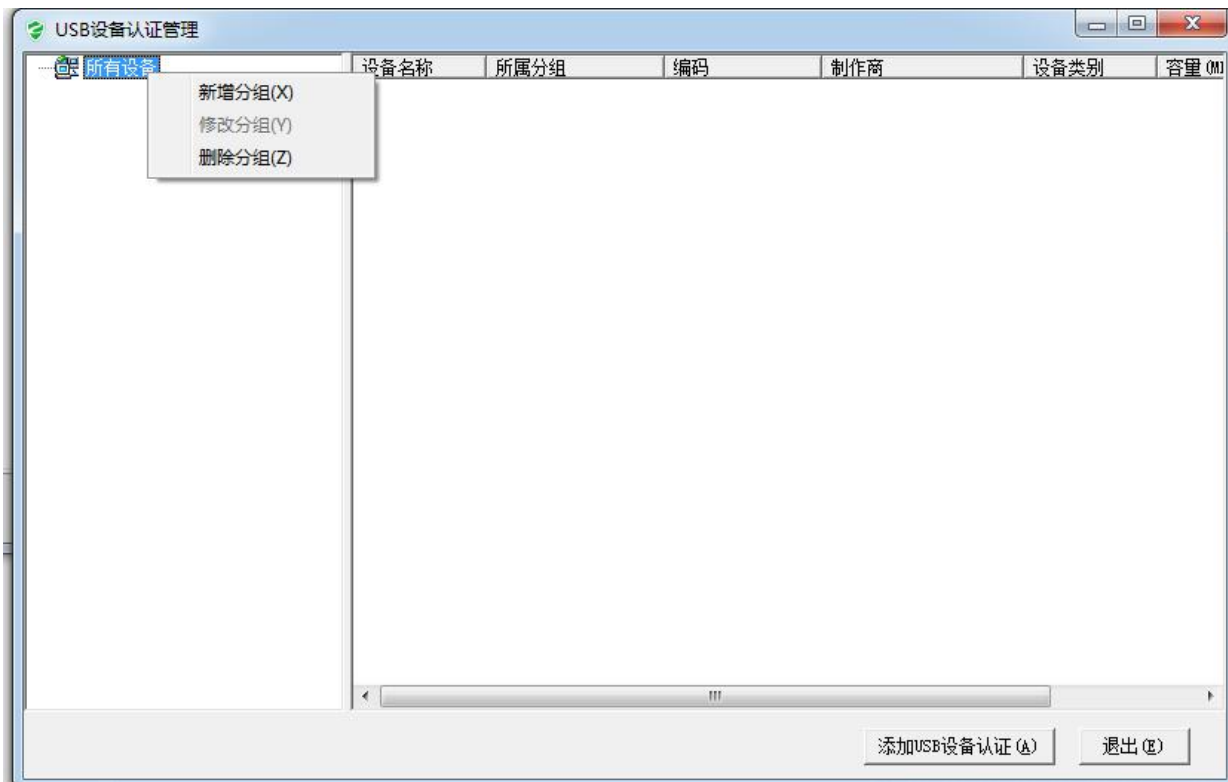
USB 存储设备认证功能是在限制使用 USB 存储设备使用的情况下，允许指定分组/终端可以正常使用（读、写）指定的 USB 存储设备，即指定分组\终端只能正常使用经过服务器认证的 USB 存储设备，没经过认证的 USB 存储设备将不能使用或为只读。

认证方法：

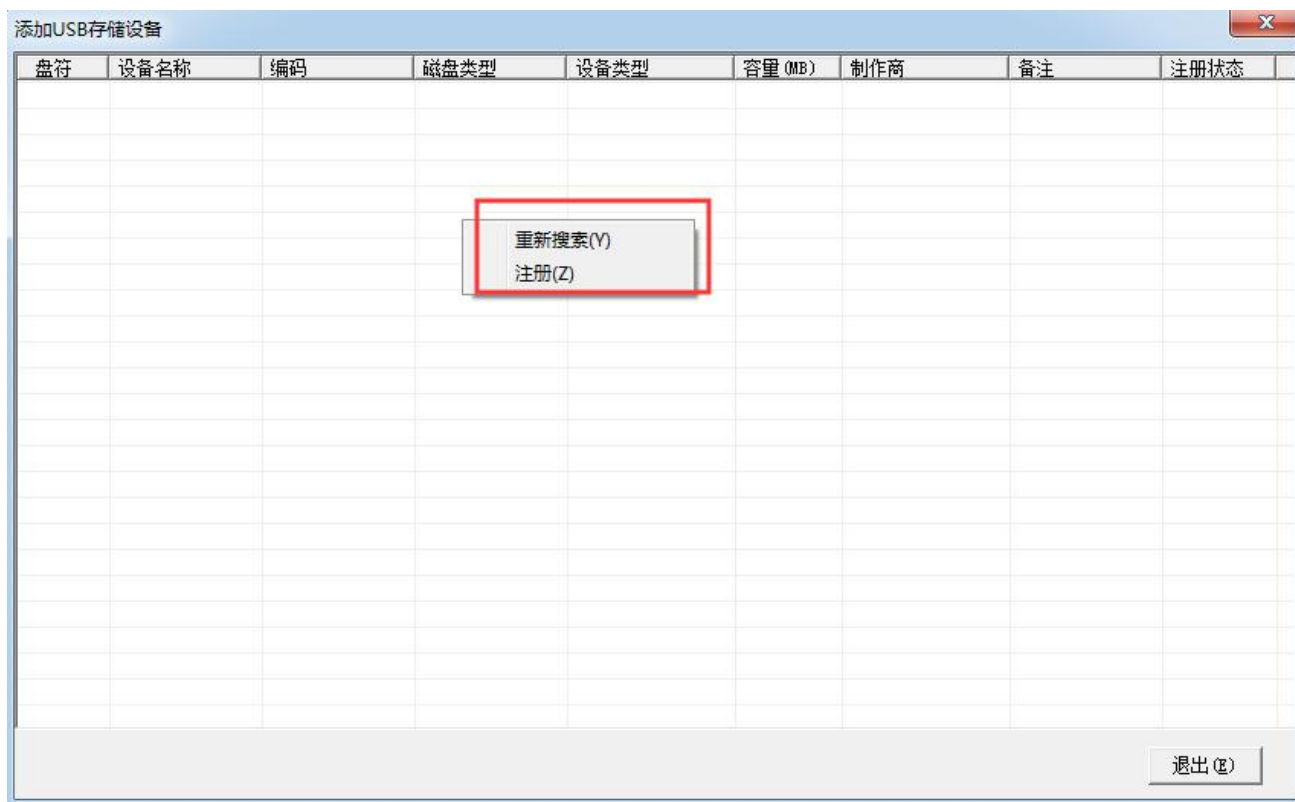
将需要认证的 USB 存储设备插在控制台电脑上，进入“USB 存储设备限制”窗口，切换到“USB 存储设备认证”页面，如下图所示。



点击“管理 USB 存储设备”按钮，弹出“USB 设备认证管理”窗口。如下图所示



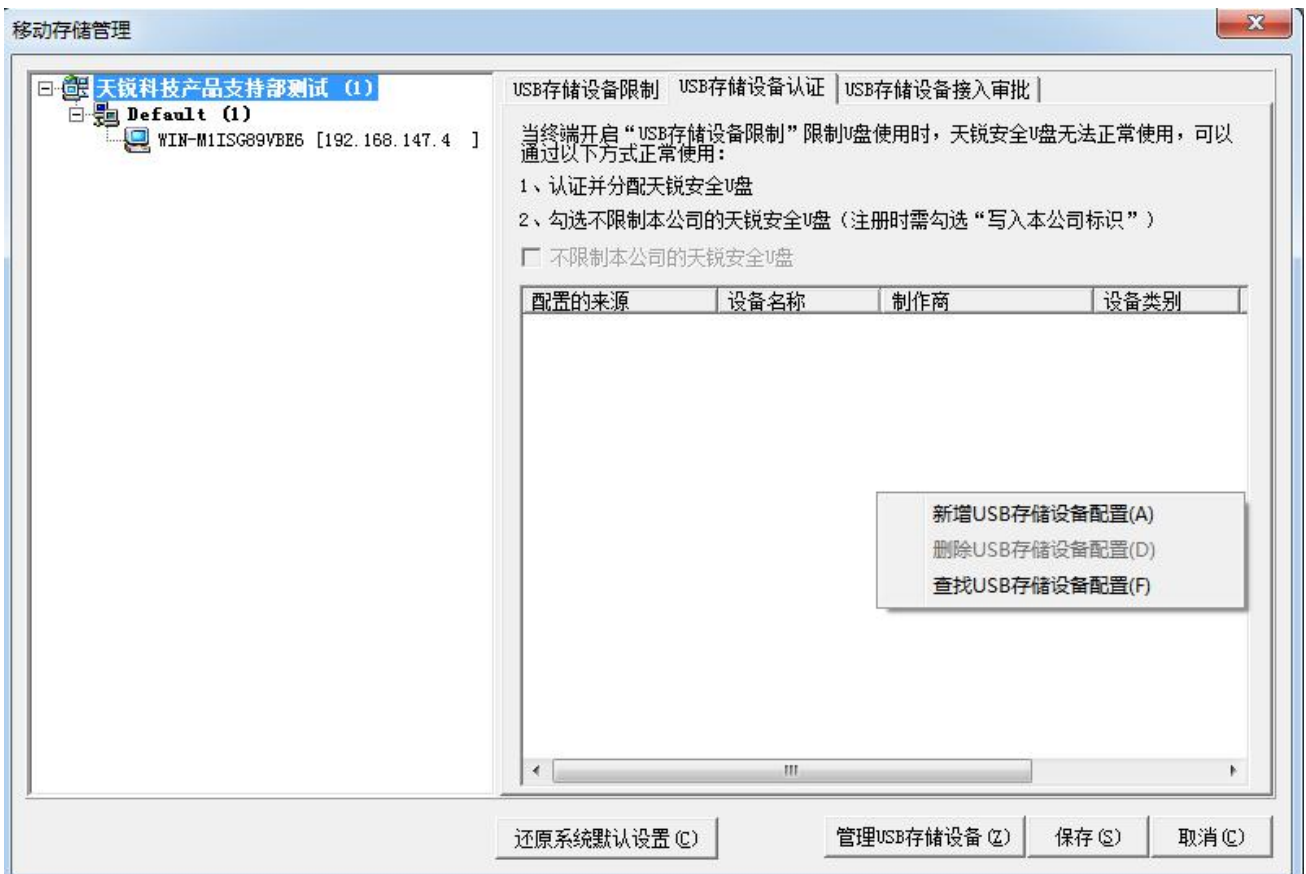
在 USB 设备认证管理界面，左边选择对应的分组，右下角点击添加 USB 设备认证。进到添加 USB 存储设备界面，可以选择对应的 U 盘右键注册，或者在空白处右键重新搜索，搜索到 U 盘后右键注册。



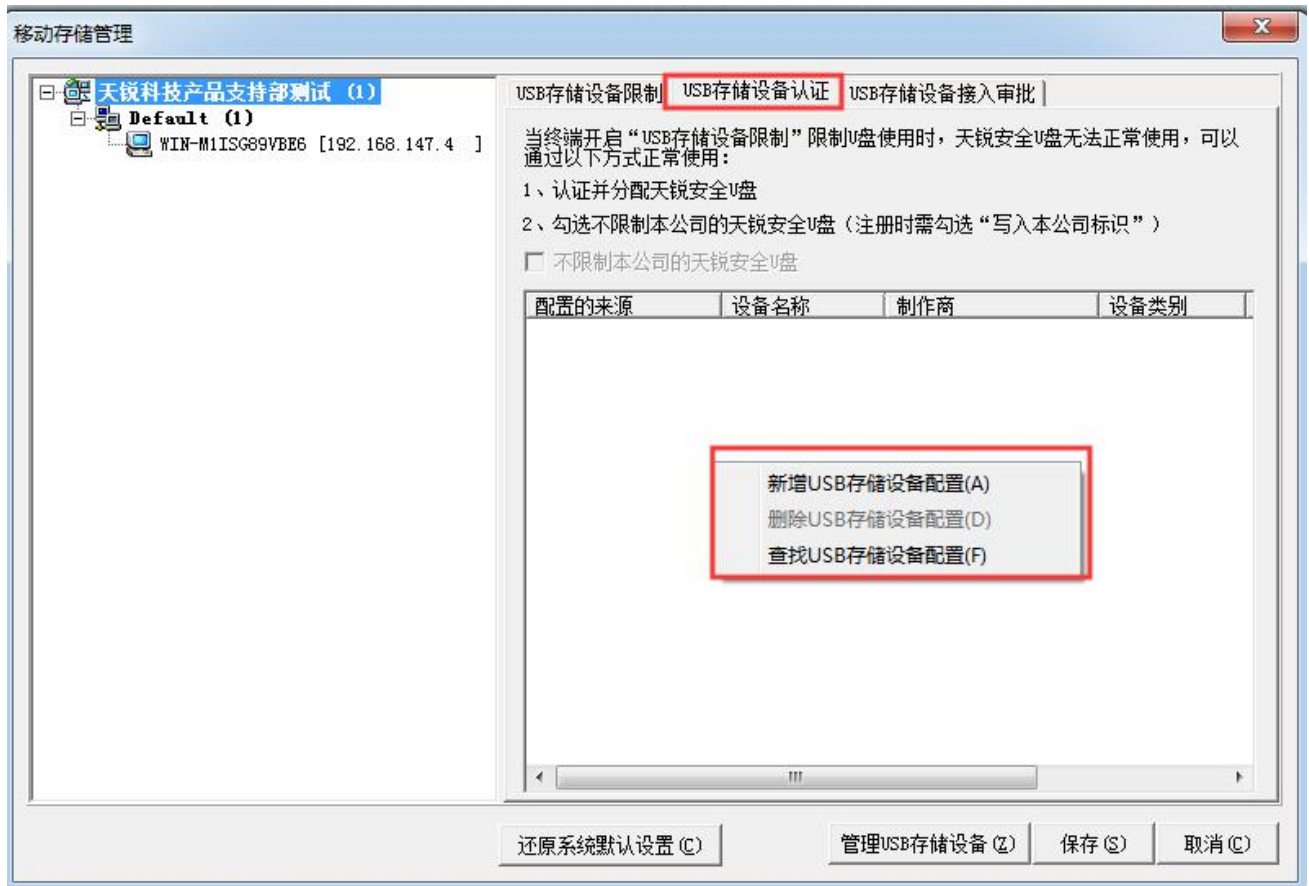
注册好后的 U 盘，可以在 USB 设备认证管理界面，右键编辑设备信息、删除设备信息和修改所属分组。



添加完 USB 设备认证后，回到移动存储管理界面，点击 USB 存储设备认证，可以选择对应的 U 盘，右键新增 USB 存储设备配置、删除 USB 存储设备配置和查找 USB 存储设备配置。



左边选择对应的公司、分组或者终端，新增 USB 存储设备配置，可以对应分配整个设备的分组或者单独一个设备（USB）。在新增 USB 存储设备配置界面，也可以添加 USB 设备认证。





查找 USB 存储设备配置。左边选择分组，右边右键点击查找 USB 存储设备配置，可以通过 USB 名称、USB 编码和制作商信息查找已配置的 U 盘。

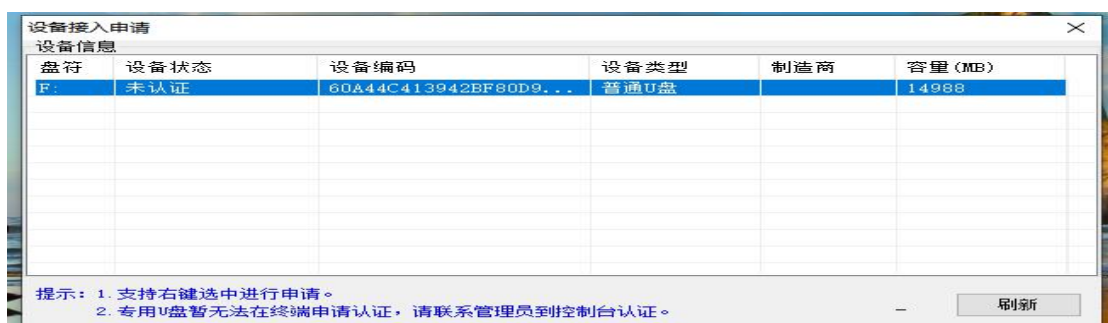


注意：USB 存储设备认证是在“USB 存储设备限制”设置为“禁止使用或只读”的情况下才生效，使USB 存储设备限制更人性化。

当终端开启“USB 存储设备限制”限制 U 盘使用时，天锐安全 U 盘无法正常使用，可以通过两种方式正常使用。（1、认证并分配天锐安全 U 盘。2、勾选不限制本公司的天锐安全 U 盘，注册时需勾选“写入公司标识”）

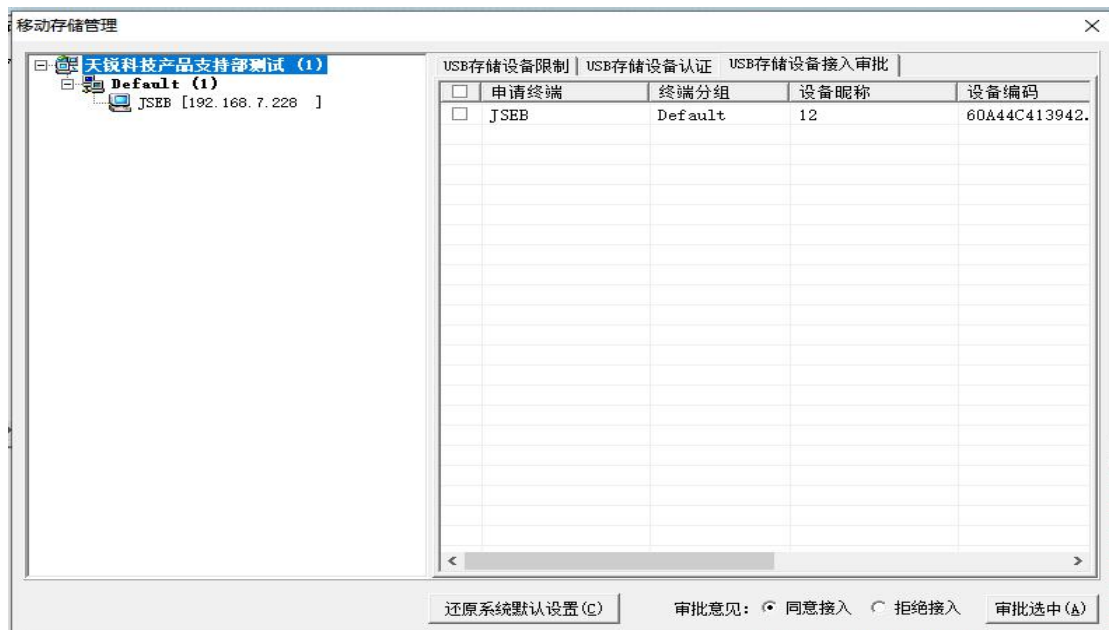
2.2.5.3 USB 存储设备接入审批

如果终端原本是被禁止使用 USB 设备的，而终端有新的 U 盘想要申请。则需要在终端插入 U 盘，鼠标左键点击右下角的绿盾图标-USB 存储设备认证申请。选择对应的 U 盘，如下图所示，填写对应的申请理由等信息，之后提交。





在控制台，USB 存储设备接入审批可以看到申请，如下图所示，勾选对应的 U 盘，审批选中，选择对应分组，点击确定即可。也可以选中对应的 U 盘，右键同意接入或者拒绝接入。

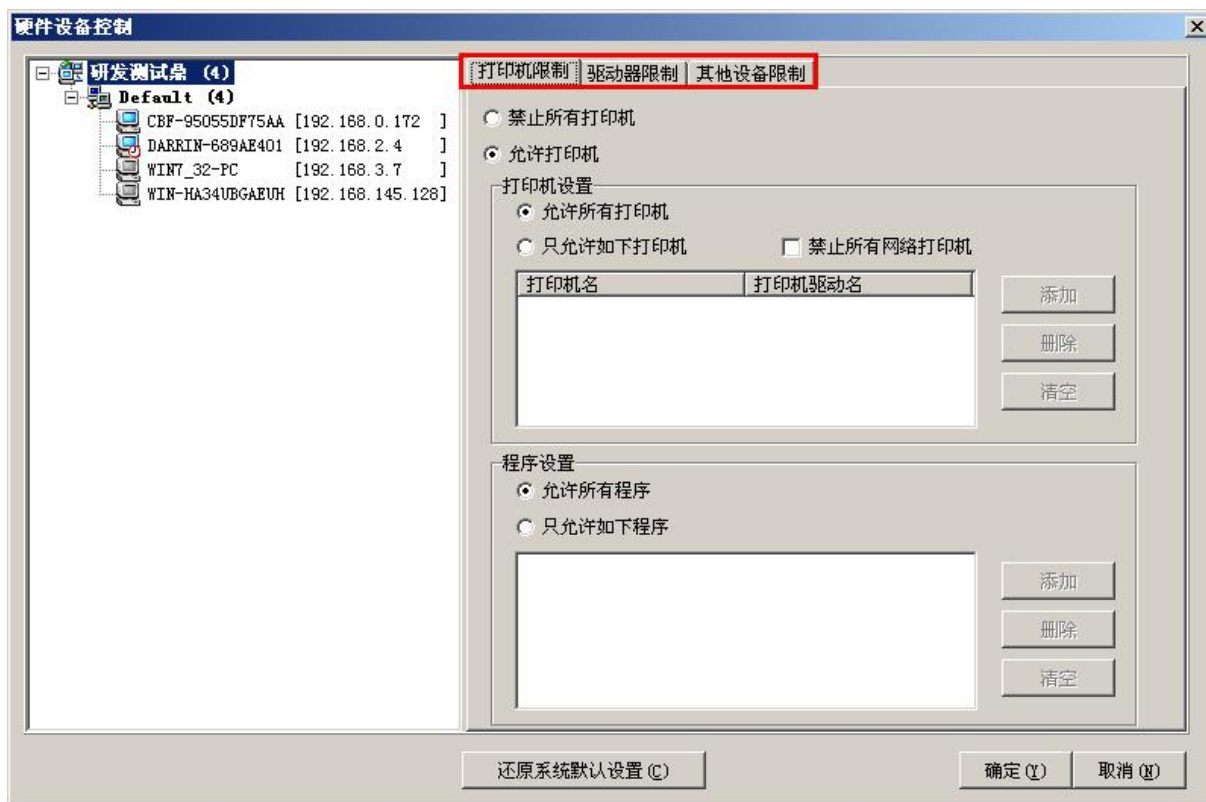


2.2.6 硬件设备控制

禁止终端使用指定设备，包括打印机限制、驱动器限制及其他设备限制。其中，打印机限制可以设置禁止所有打印机，或只允许使用指定打印机、只允许指定程序使用打印机；驱动器限制包括光盘驱动器限制、软盘驱动器限制，可以设置成允许使用、禁止使用或只读，并可以按照时间规则限制；可以限制串口、并口、红外线、蓝牙、modem、键盘、鼠标、网卡、声音等设备的使用。

在控制台的功能栏选择“策略管理”-“硬件设备限制”，在弹出的“硬件设备控制”窗口左侧选择需要限制的对象（可以选择公司名称、分组或终端），在窗口右侧勾选需要限制的

内容。硬件设备限制支持继承，只要公司名称、分组或终端一个地方设置了限制，该限制规则即生效。如下图所示（以打印机限制为例）：



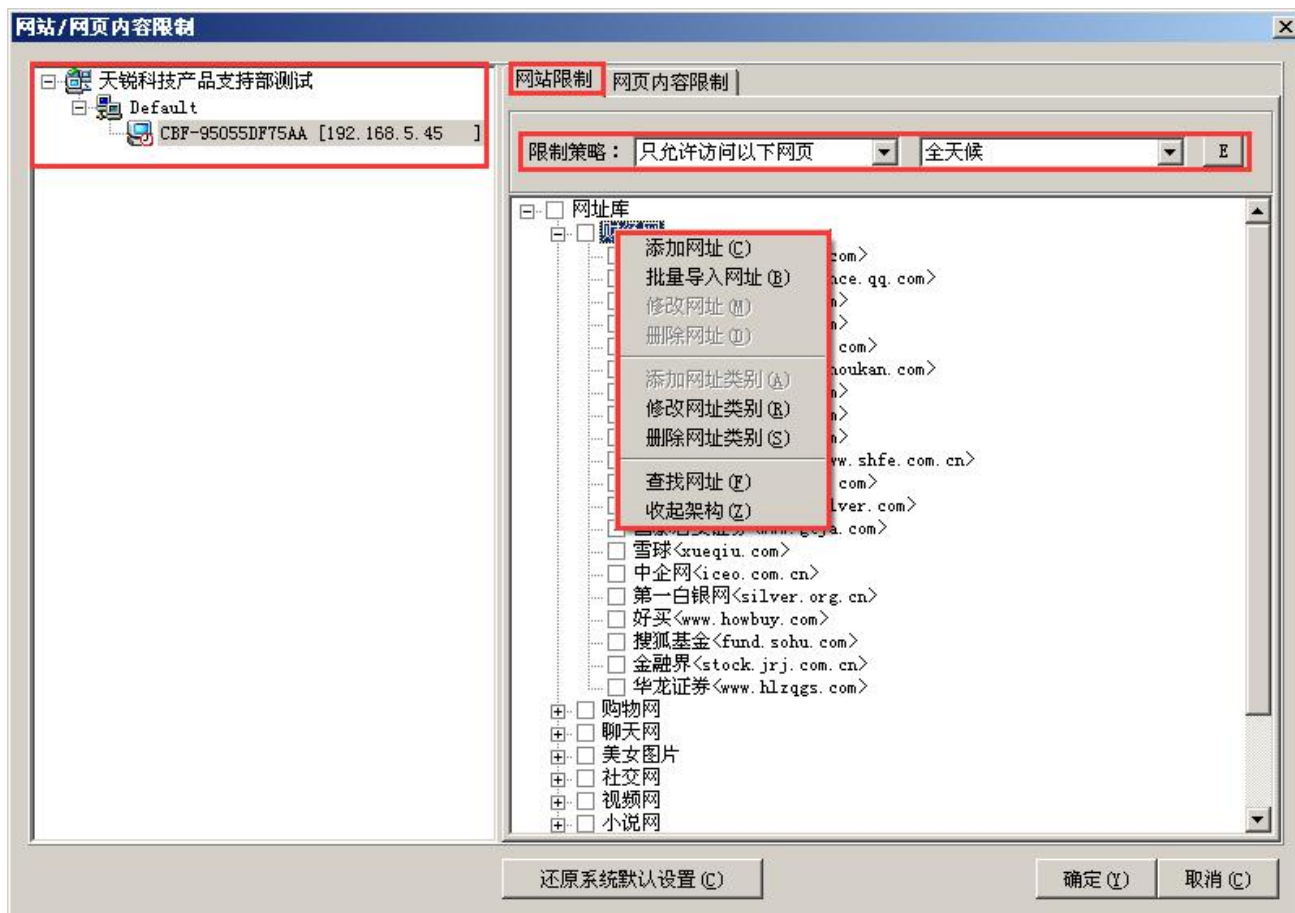
2.2.7 网站/网页内容限制

可以对终端的网页浏览行为进行限制，可以设置禁止/只允许浏览指定网站、禁止访问所有网页以及网页关键字限制。



2.2.7.1 网站限制

在控制台的功能栏选择“策略管理”-“网站/网页内容限制”，在弹出的“网站/网页内容限制”窗口选择“网站限制”选项，左侧选择需要限制的对象（可以选择公司名称、分组或终端），窗口右侧选择网页浏览的限制策略，可以点击“E”按钮设置限制策略的生效时间，再在网址库中选择限制策略的指定网站。如下图所示：



在网址库中，系统默认自带一些常用的分类网址，管理员根据实际需要，可以添加、批量导入、修改或删除网址，也可以增加、修改或删除网址类别。支持通过网站 URL、名称来快速查找网址库内的网址。

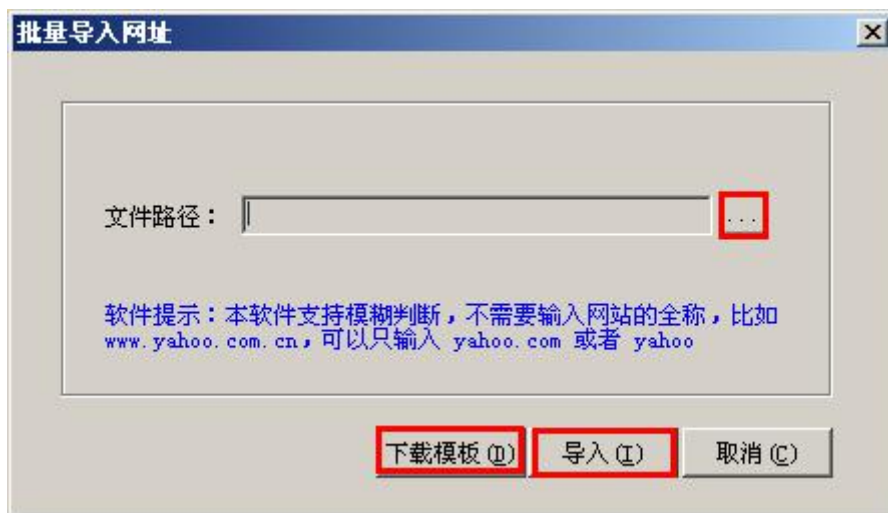
添加网址（支持 HTTP/HTTPS 协议）

选择要增加网址的类别，然后鼠标右击选择“添加网址”菜单，弹出“添加网址”窗口，在“网站名称”、“网站 URL”和“备注”栏处输入正确的数据。网站 URL 支持模糊匹配，可以不用输入前缀“http://”，不需要输入网站的全称，如要限制 QQ 空间，在“网站 URL”输入“qzone”即可。如下图所示：



批量导入网址

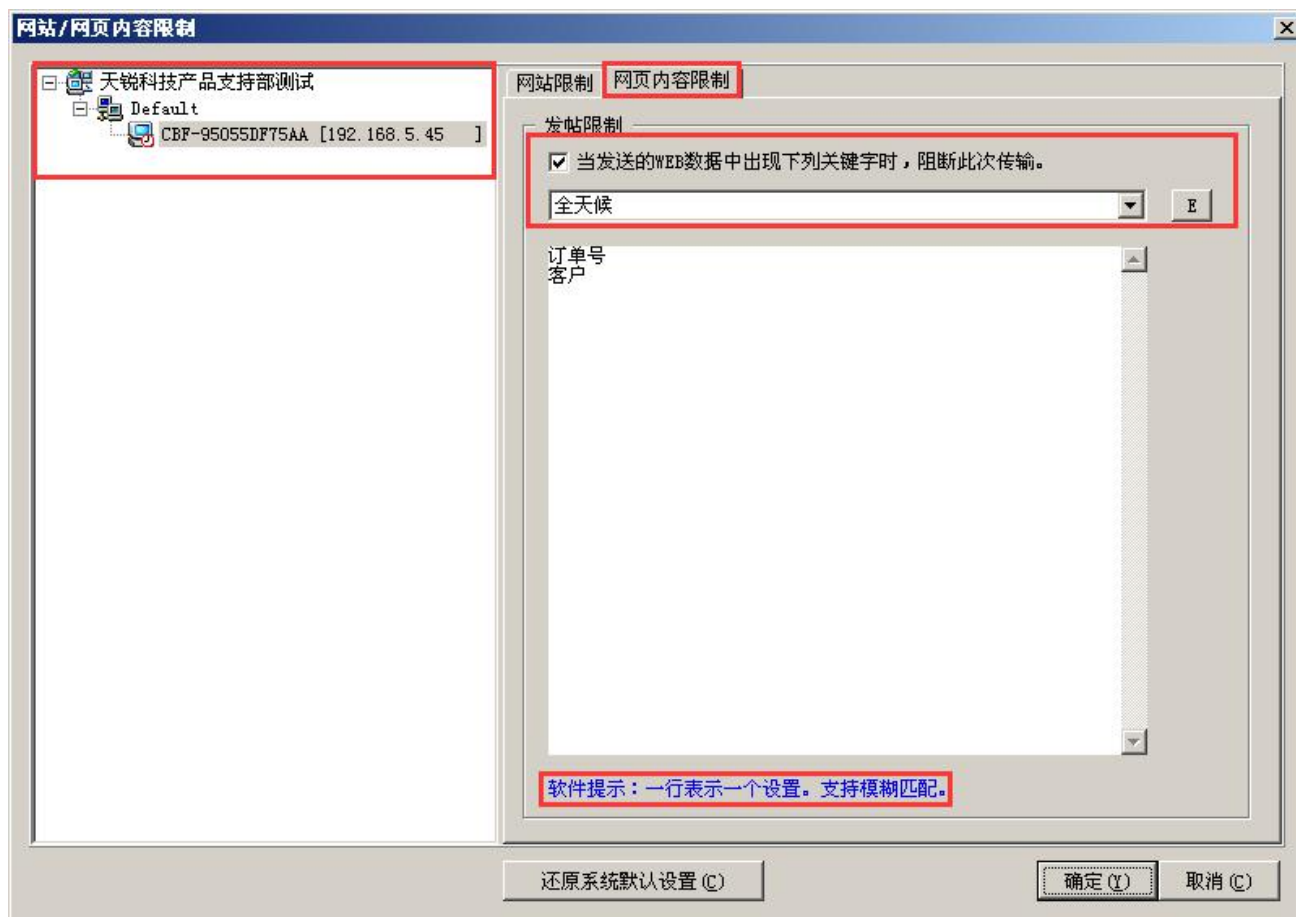
在网址库区域内，鼠标右击选择“批量导入网址”菜单，弹出“批量导入网址”窗口，点击“下载模板”按钮下载网址库模板文件，并按照该模板文件里的格式，填写要添加的网站类别、名称、URL 和备注，编辑完成后保存该模板文件。在“批量导入网址”窗口，点击“文件路径”后的“...”操作，选择刚制作的网址库文件，然后点击“导入”按钮即可。如下图所示：



2.2.7.2 网页内容限制

在控制台的功能栏选择“策略管理”-“网站/网页内容限制”，在弹出的“网站/网页内容

限制”窗口选择“网页内容限制”选项，左侧选择需要限制的对象（可以选择公司名称、分组或终端），窗口右侧勾选“当发送的WEB数据中出现下列关键字时，阻断此次传输”选项，可以点击“E”按钮设置限制策略的生效时间，再在左下方输入栏中填写要限制的关键字。如下图所示：



2.2.8 聊天工具白名单

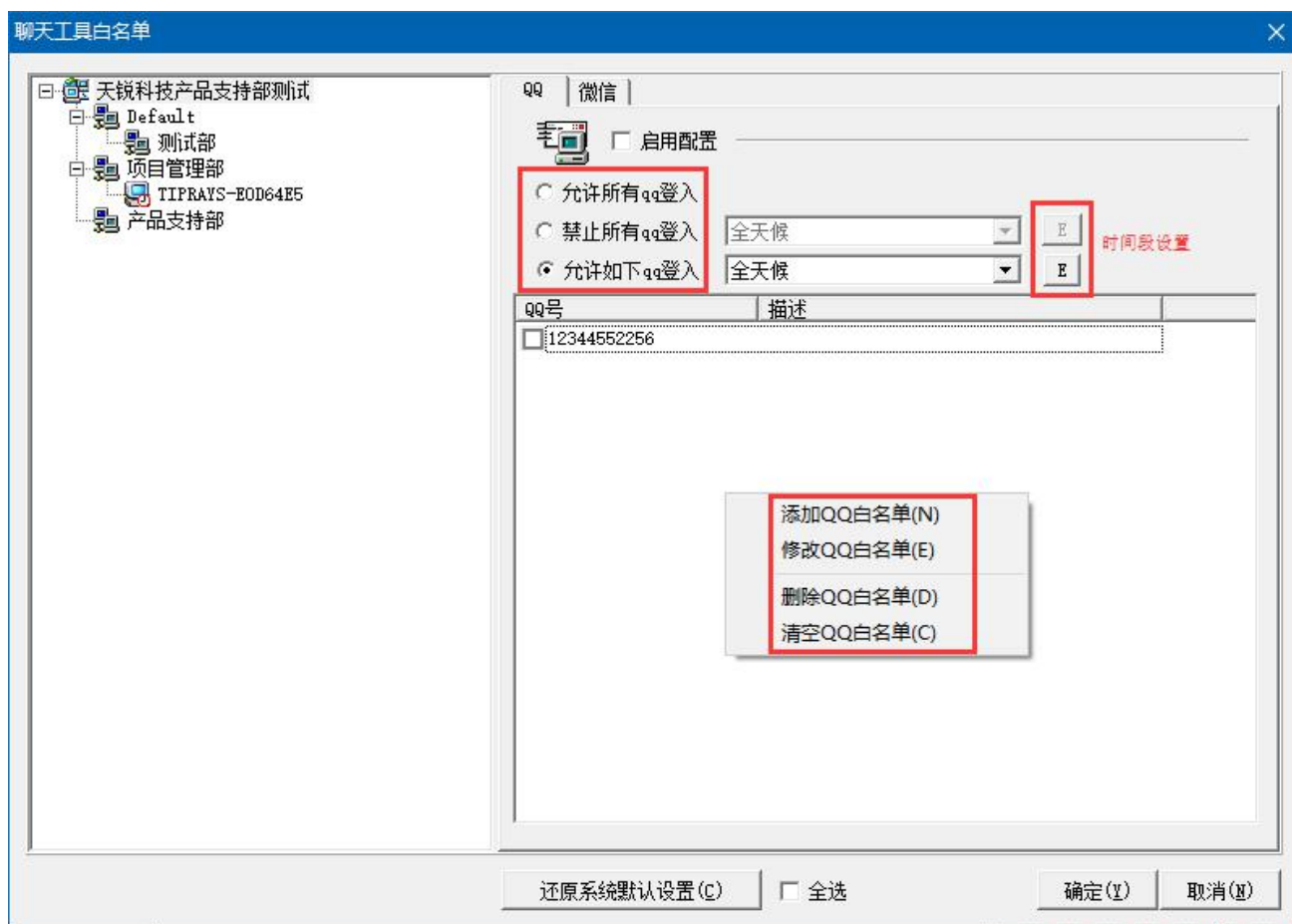
目前聊天工具白名单支持QQ以及微信软件，下面以设置QQ白名单操作为例。

设置QQ白名单，终端用户只能使用白名单中的QQ号。白名单设置支持按时间段进行管理控制，超出时间段，限制无效。

在控制台的功能栏选择“策略管理”-“聊天工具白名单”，弹出“聊天工具白名单”窗口，选择“允许如下qq登入”，再右键单击窗口右侧的空白处，在弹出的菜单项中选择“添加QQ白名单”，在“QQ信息”窗口中输入需要允许的QQ号码及其描述。

QQ白名单添加完毕之后，就可以进行配置。在“QQ白名单设置”窗口左侧的用户列表中选择要限制的分组或终端用户，在窗口右侧选择“启用配置”，再选择要限制的选项，如果

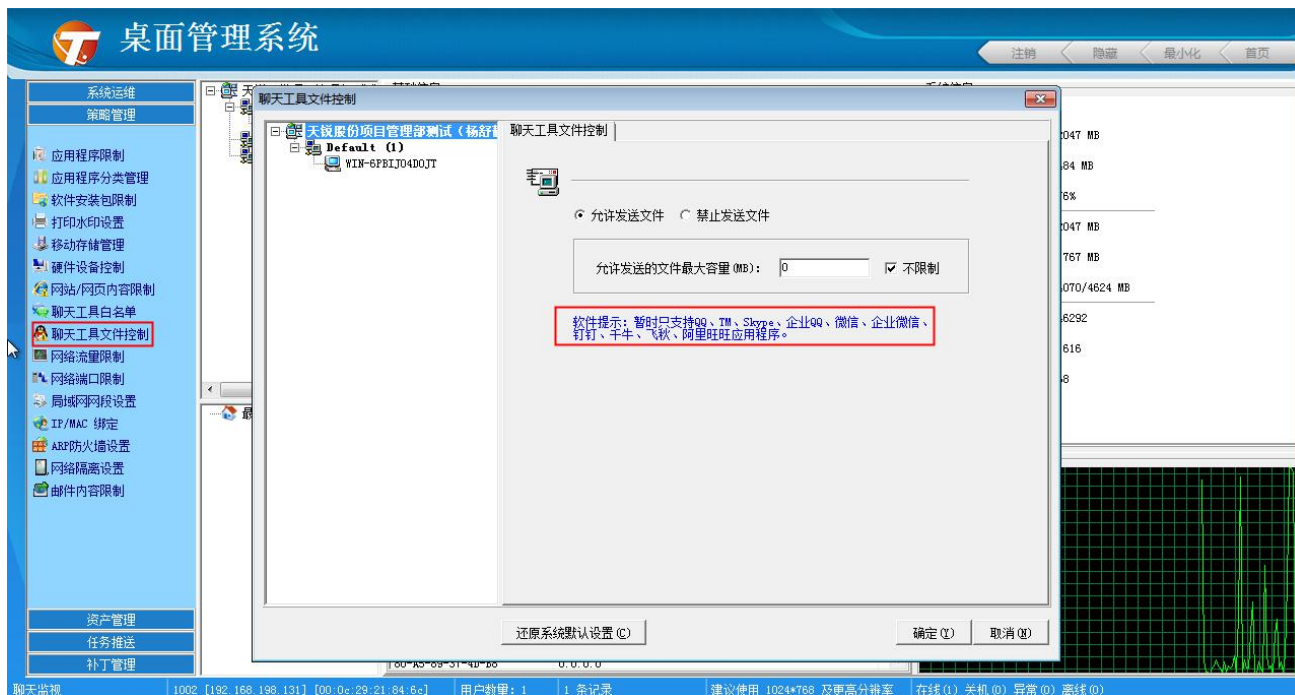
只允许指定 QQ 登入，还要在 QQ 列表中勾选相应的 QQ 白名单号码。设置完毕，确定即可。
如下图所示：



2.2.9 聊天工具文件控制

可以设置终端电脑允许/禁止发送文件，并且允许发送文件时可以限定终端电脑允许发送的文件最大容量，超过设定值不能发送。目前暂支持 QQ、TM、Skype、企业 QQ、微信、企业微信、钉钉、千牛、飞秋、阿里旺旺应用程序。

在控制台的功能栏选择“策略管理”-“聊天工具文件控制”，弹出“聊天工具文件控制”窗口，窗口左侧选择需要限制的对象（可以选择公司名称、分组或终端），窗口右侧设置策略，设置完成后点击确定即可。如下图所示：



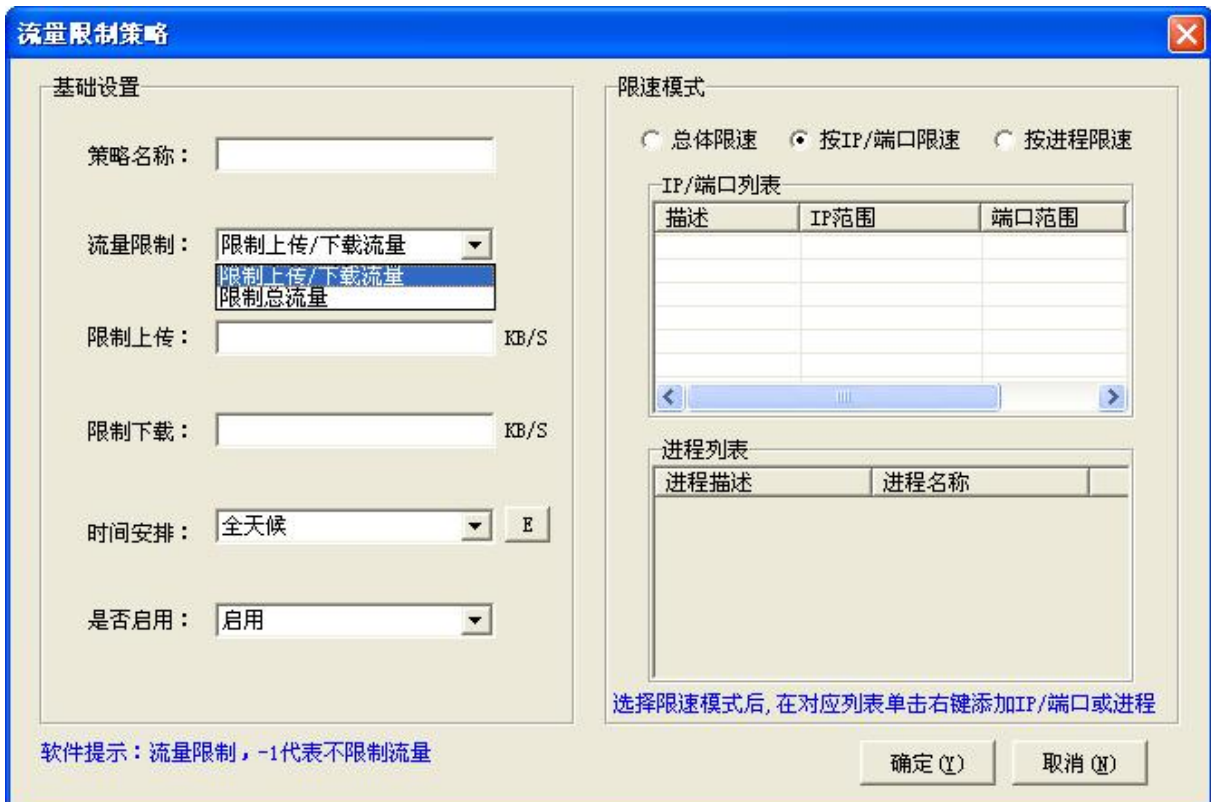
2.2.10 网络流量限制

对公司的网络资源进行合理分配。可结合流量观察、统计功能，对大流量的终端用户的上网流量，包括上传流量、下载流量或总流量进行限制，使网络资源得到有效利用。流量限制支持按时间段设置，如相应的流量限制策略只在上班时间内生效。

在控制台的功能栏选择“策略管理”-“网络流量限制”，弹出“网络流量限制”窗口。如下图所示。系统默认自带了三个分别按总体、按 IP/端口、按进程限速的策略，可以自行再添加、修改、删除策略，并分配策略。



鼠标左键单击窗口右下侧的“添加策略”按钮（或者在窗口右侧空白处右键鼠标选择），弹出“流量限制策略”设置窗口，如下图所示：



“策略名称”：要添加的策略名称，以区别于其他策略；

“流量限制”：选择是分别对上传/下载流量进行限制，还是限制总流量；

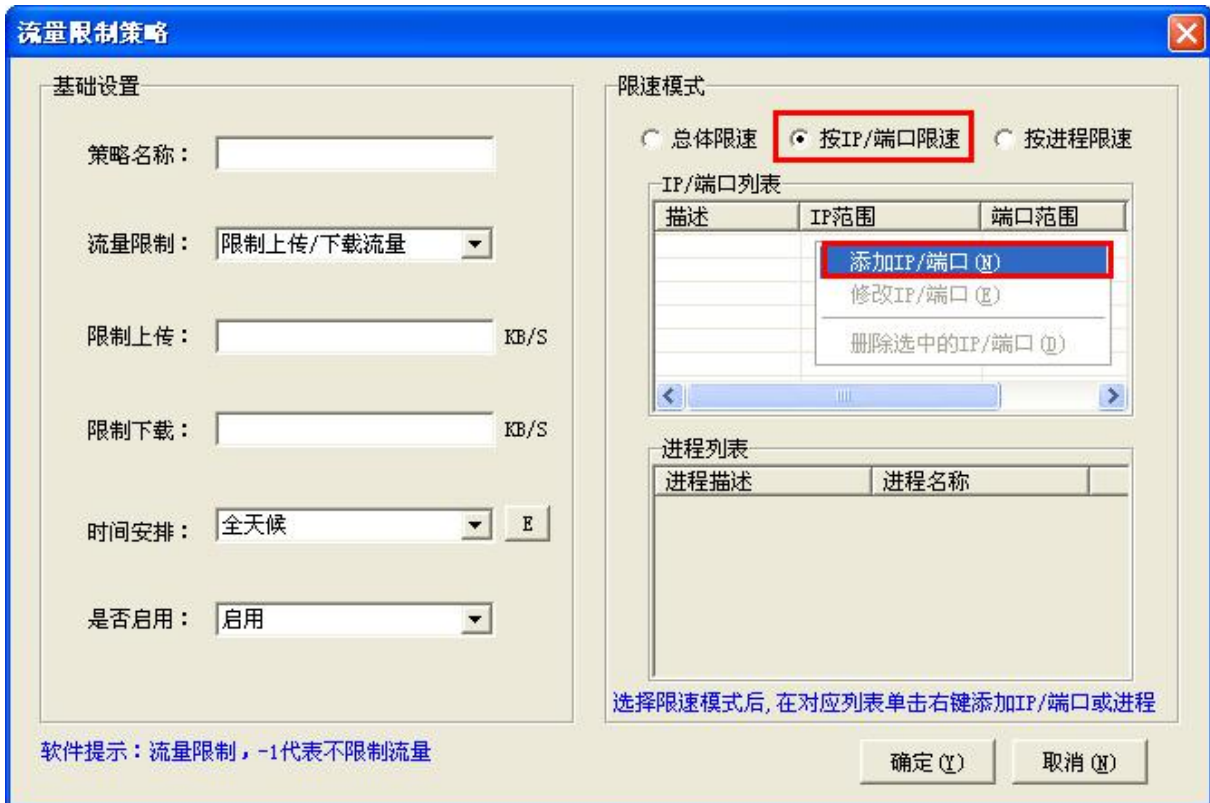
“限制上传/下载/总流量”：要限制的流量值，单位为 KB/S；

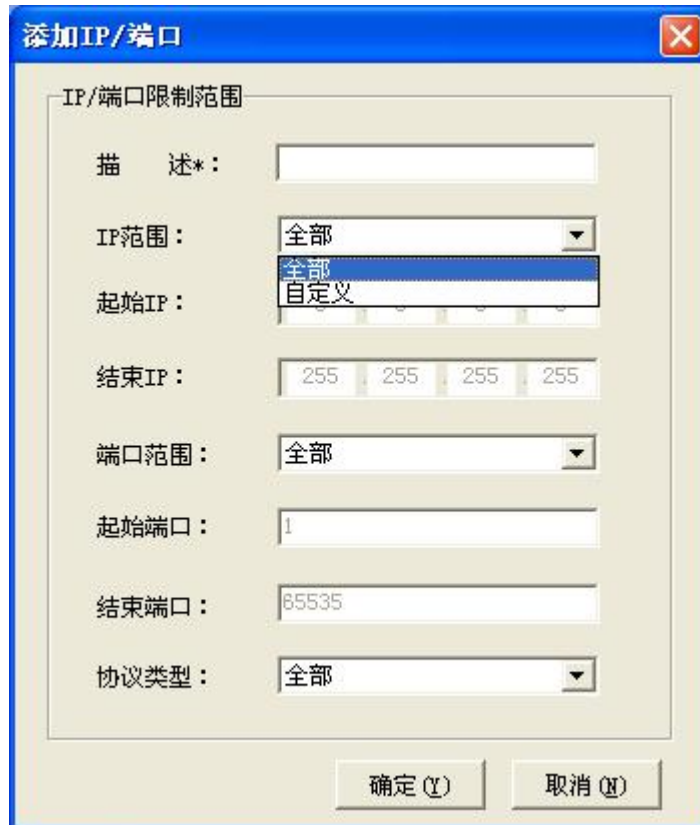
“时间安排”：该策略在什么时间段内生效，如全天或上班时间内生效；

“是否启用”：启用或禁用策略，启用时该策略生效；

“限制模式”包含三种：总体限速、按 IP/端口限速和按进程限速。默认为总体限速。

- 总体限速：限制策略对所有 IP、端口及进程生效。
- 按 IP/端口限速：限制策略只对指定的 IP 和端口生效。选择“按 IP/端口限速”限速模式，“IP/端口列表”变为可编辑状态。右键鼠标进行策略的添加、修改和删除。





该对话框用于配置IP/端口限制范围。其包含以下字段：

- 描述*：** 文本输入框，用于输入描述。
- IP范围：** 下拉菜单，当前显示“全部”，下方有“全部”和“自定义”两个选项。
- 起始IP：** 文本输入框，当前显示“自定义”。
- 结束IP：** 四个数字输入框，分别显示“255”、“255”、“255”、“255”。
- 端口范围：** 下拉菜单，当前显示“全部”。
- 起始端口：** 文本输入框，当前显示“1”。
- 结束端口：** 文本输入框，当前显示“85535”。
- 协议类型：** 下拉菜单，当前显示“全部”。

底部有两个按钮：“确定(Y)”和“取消(N)”。

“描述”：IP/端口限制范围描述，自定义，以区别于其他IP/端口限制范围；

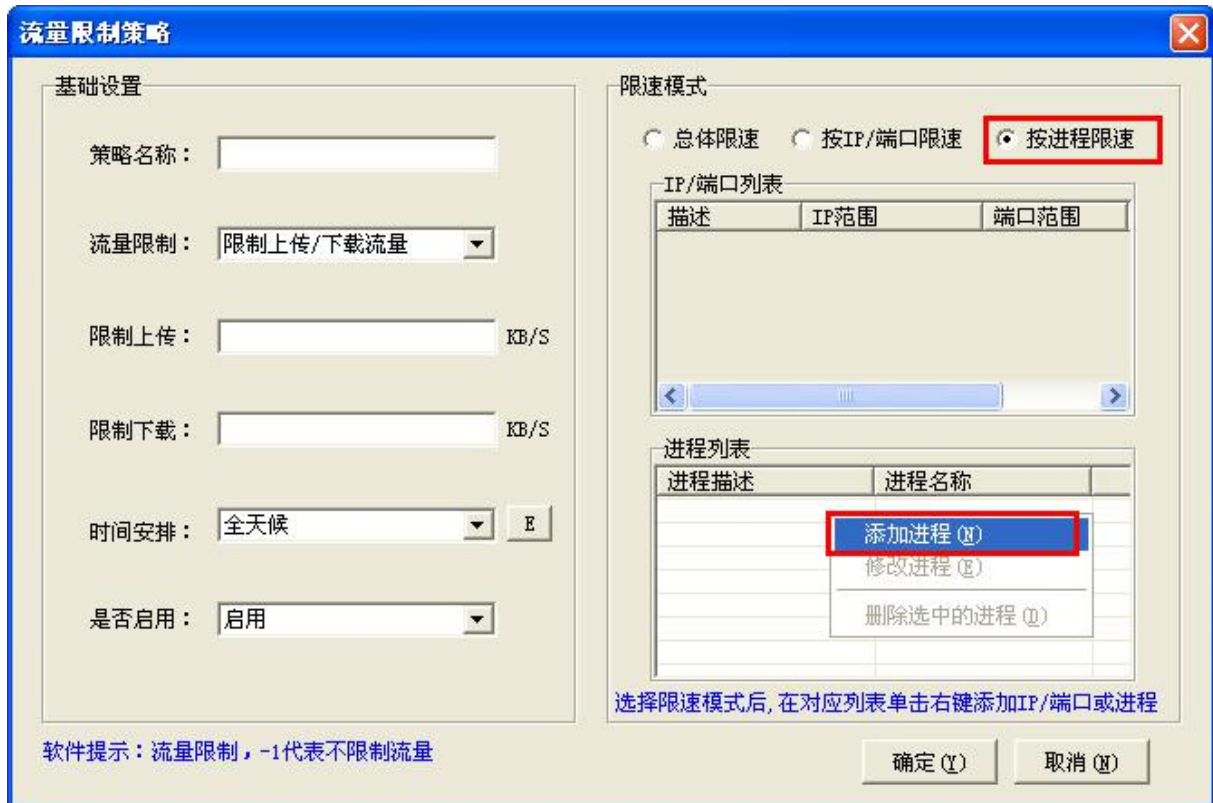
“IP/端口范围”：全部IP/端口，或需要自定义IP/端口范围；

“起始IP/端口”：需要限制的起始IP/端口号；

“结束IP/端口”：需要限制的结束IP/端口号；

“协议类型”：需要限制的协议，TCP、UDP 或全部。

● **按进程限速：**限制策略只对指定的进程生效。选择“按进程限速”限速模式，“进程列表”变为可编辑状态。右键鼠标进行策略的添加、修改和删除。



“进程描述”：要添加的限制进程描述，自定义；

“进程名称”：需要限制的进程名称，可以点击“...”按钮浏览本地可执行文件添加。

策略配置完成后，再进行策略分配。在“流量限制”窗口左侧选择需要限制的对象（可以选择公司名称、分组或终端），窗口右侧选择相应策略后确定即可。

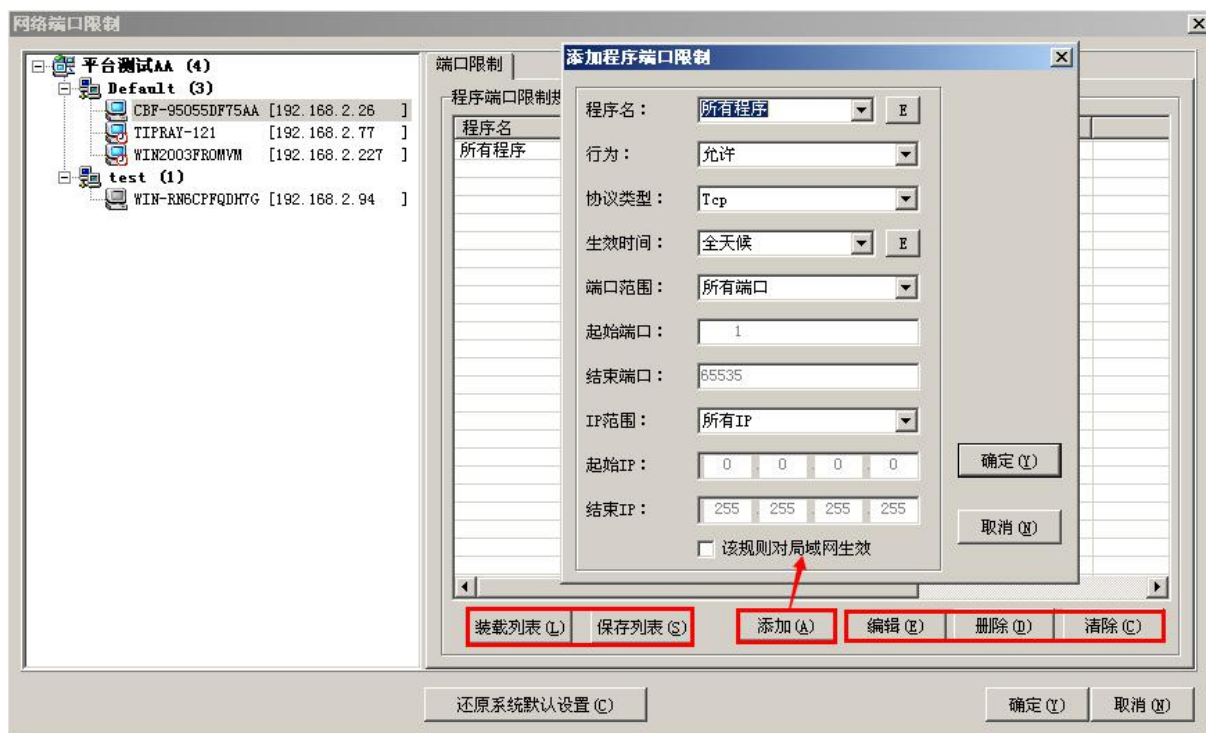
鼠标右键点击策略，选择“已分配的对象”，可以查看该策略已运用于哪些分组及终端。如下图所示。去掉分组/终端前的复选项，并点击“修改”按钮，可以取消策略对该对象的分配。



2.2.11 网络端口限制

限制终端的网络端口，可以按程序名、协议类型、端口范围、IP 范围等进行限制。

在控制台功能栏选择“策略管理”-“网络端口限制”，在弹出的“网络端口限制”窗口左侧选择需要限制的对象（可以选择公司名称、分组或终端），在窗口右侧点击“添加”按钮，在弹出的“添加程序端口限制”窗口中进行端口配置。配置的端口列表信息可以导出（“保存列表”）为文档保存，供下次恢复配置使用（“装载列表”）。每个端口限制都可以单独设置生效时间。如下图所示：



说明:此功能支持 Windows 和 Mac 终端。

注意：如果在网络端口限制中勾选了“该规则对局域网生效”，那么即使在“局域网网段设置”中进行相应设置，也是无效的。

2.2.12 局域网网段限制

当前企业的局域网建设越来越庞大，也越来越复杂，同个企业存在不同的网段。而增加局域网网段设置，有效的区分该端口限制是否对局域网网段生效，同时可以过滤访问局域网网段产生的流量不纳入统计。在控制台的功能栏选择“策略管理”-“局域网网段设置”，点击“添加”按钮进行添加。如下图所示：

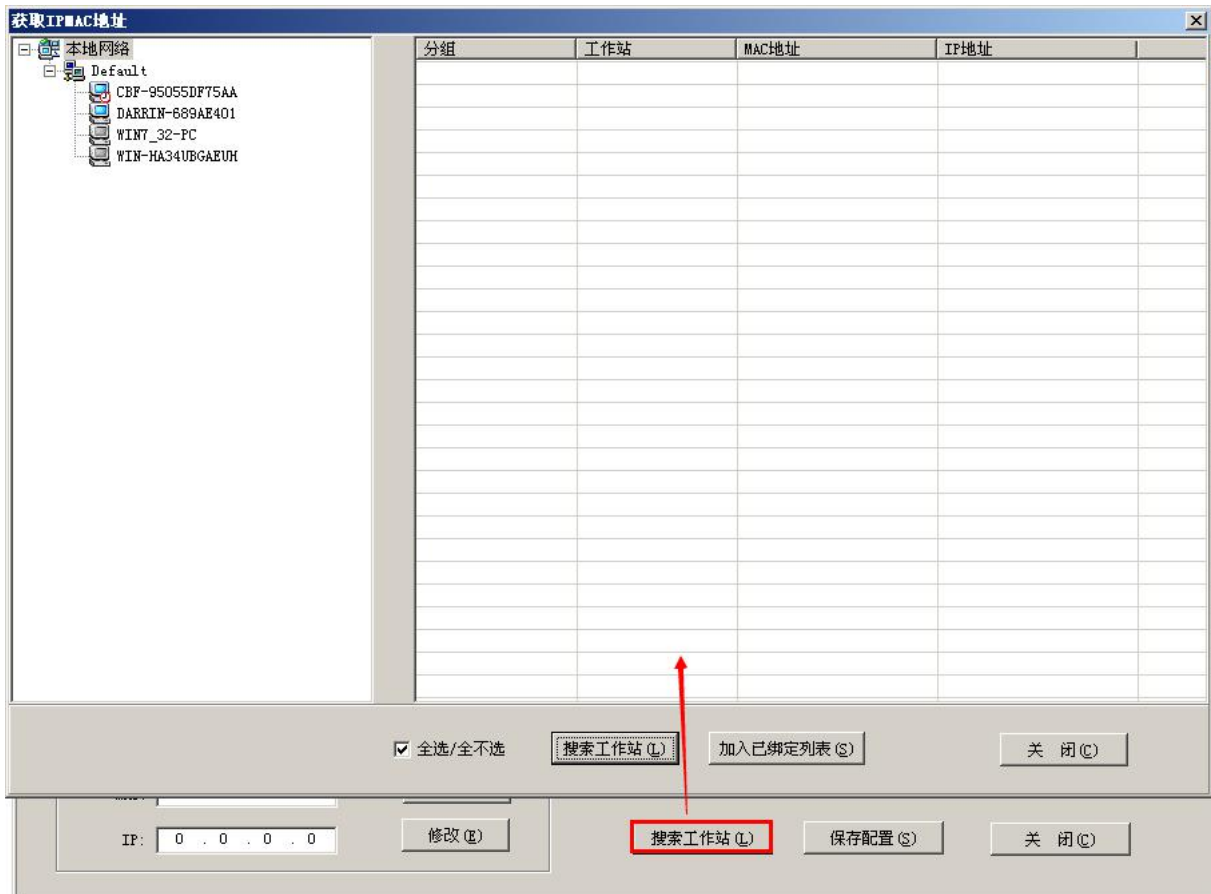


注意：如果在网络端口限制中勾选了“该规则对局域网生效”，那么即使在“局域网网段设置”中进行相应设置，也是无效的。

2.2.13 IP/MAC 绑定

可以对终端电脑的 IP 地址和 MAC 地址进行绑定，防止终端随意更改。如果设置了 IP/MAC 绑定，终端电脑的 IP 或者 MAC 地址改变，系统就会切断该计算机的网络连接，使其不能上网。该操作是针对安装天锐绿盾终端的计算机有效。

在控制台的功能栏选择“策略管理” - “IP/MAC 绑定”，在弹出的“IP/MAC 绑定”窗口中点击“搜索”按钮，弹出“获取 IP/MAC 地址”窗口，点击该窗口的“搜索工作站”按钮，系统会自动获取在线终端的 IP/MAC 地址，搜索完毕，勾选需要绑定的 IP/MAC 地址“加入已绑定列表”，返回“IP/MAC 绑定”窗口，点击“保存”即可。也可以在“MAC 地址绑定”窗口的左下角手动选择终端，并输入相应的 MAC、IP 来绑定。如下图所示：



说明:此功能支持 Windows 和 Mac 终端。

2.2.14 ARP 防火墙设置

ARP 防火墙可以有效地防止终端受 ARP 欺骗攻击以及因局域网内 ARP 病毒引起的网络故障。

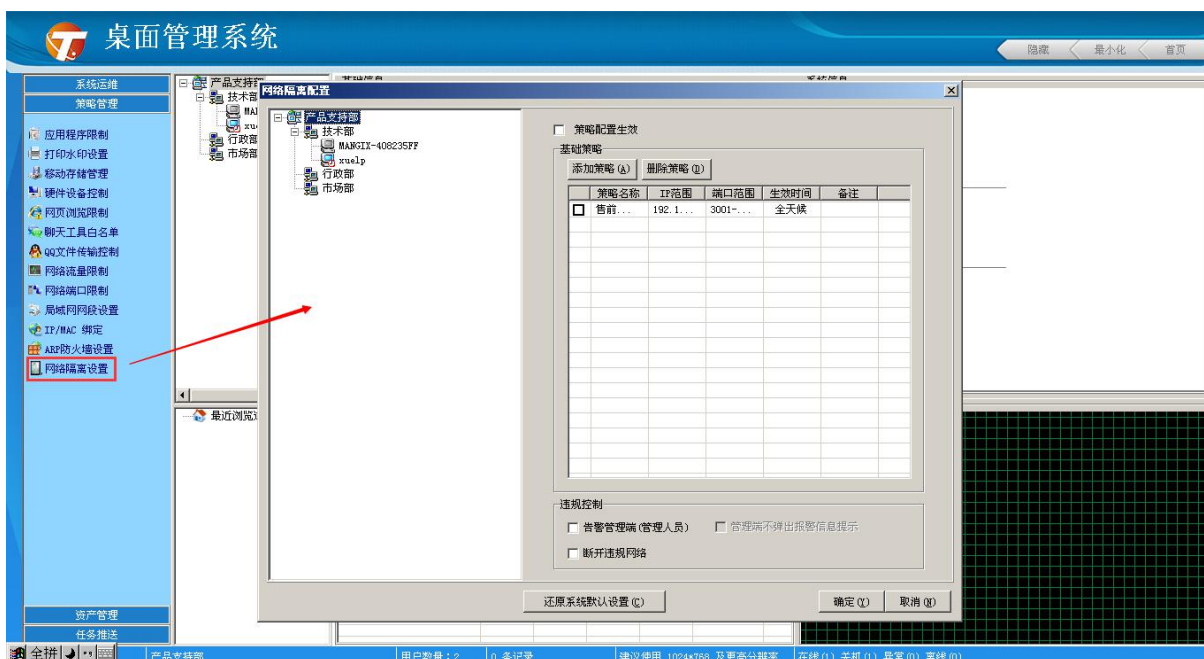
在控制台的功能栏选择“策略管理”-“ARP 防火墙设置”，在弹出的窗口中，手动填写要绑定的终端的 IP 地址，点击“IP-MAC”按钮，获取终端 MAC 以后，点击“添加到列表”按钮，依次添加各终端的 IP 和 MAC 信息，即完成绑定配置。添加完毕点击“保存配置”按钮。如下图所示：



2.2.15 网络隔离设置

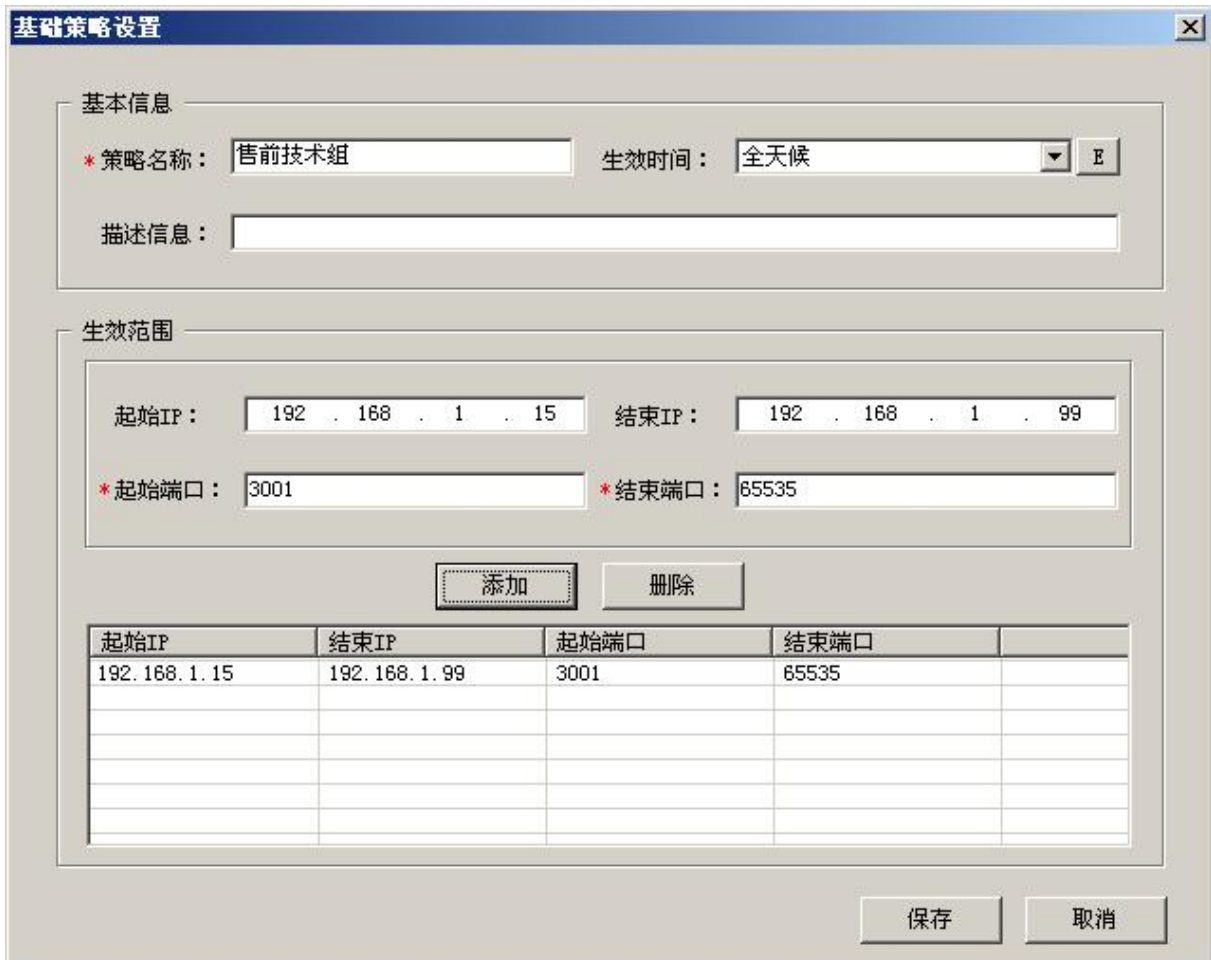
当网络被隔离时，某部门或终端用户去访问指定范围外的 IP 地址和端口号时，会被禁止访问，这样可以杜绝计算机违规外联的可能，保障了涉密内网的安全。

在控制台的功能栏选择“策略管理”-“网络隔离设置”，弹出“网络隔离配置”窗口。如下图所示：



添加策略

在窗口右侧点击“添加策略”按钮，弹出“基础策略设置”窗口，进行策略设置，可以配置策略的生效时间，还支持创建多条 IP 和端口范围。设置完成后，点击“保存”按钮。如下图所示：



基础策略设置窗口包含以下信息：

基本信息

* 策略名称：售前技术组 生效时间：全天候

描述信息：

生效范围

起始IP：192 . 168 . 1 . 15 结束IP：192 . 168 . 1 . 99

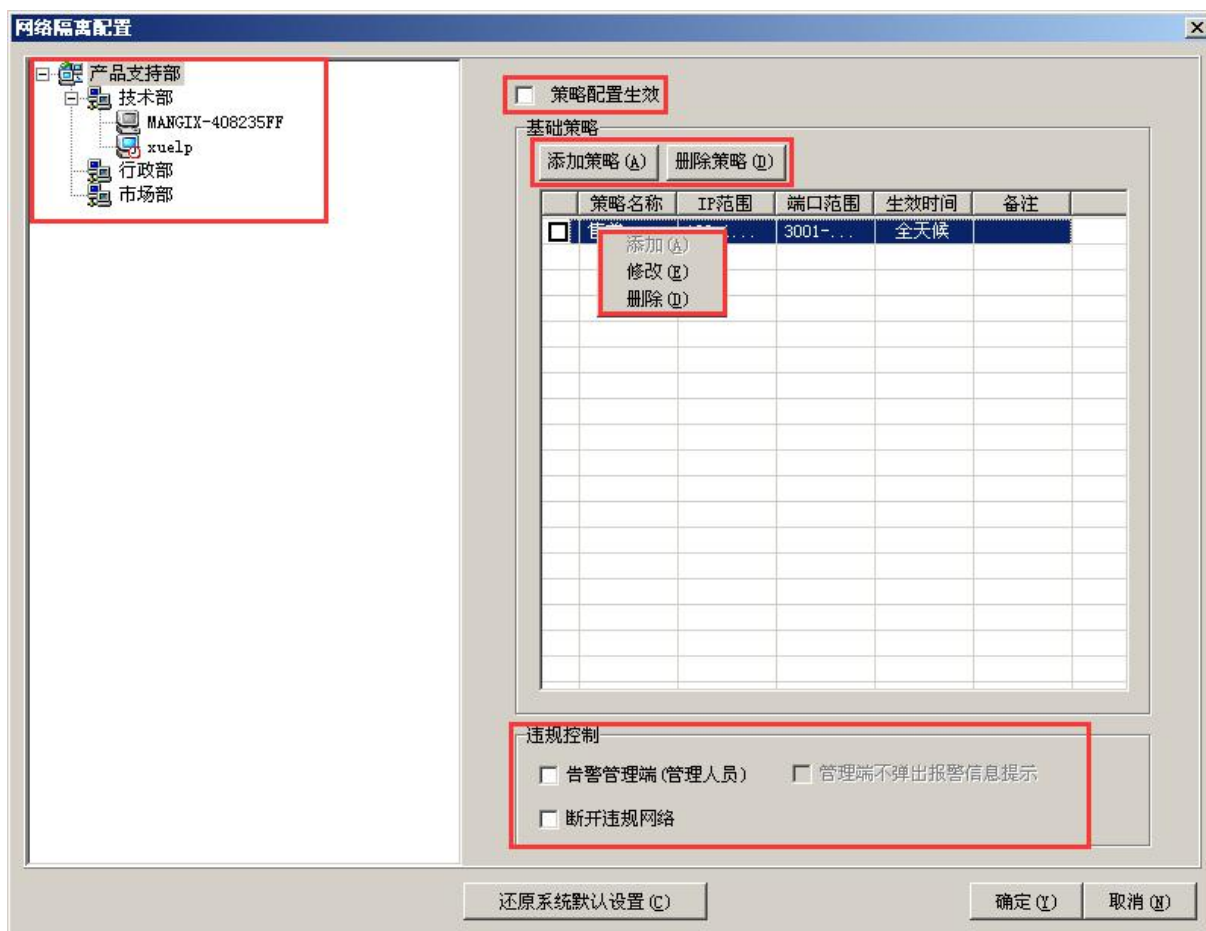
* 起始端口：3001 * 结束端口：65535

添加 删除

| 起始IP | 结束IP | 起始端口 | 结束端口 |
|--------------|--------------|------|-------|
| 192.168.1.15 | 192.168.1.99 | 3001 | 65535 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

保存 取消

添加好策略后，策略将显示在基础策略表中，可对其进行修改和删除操作。



分配策略

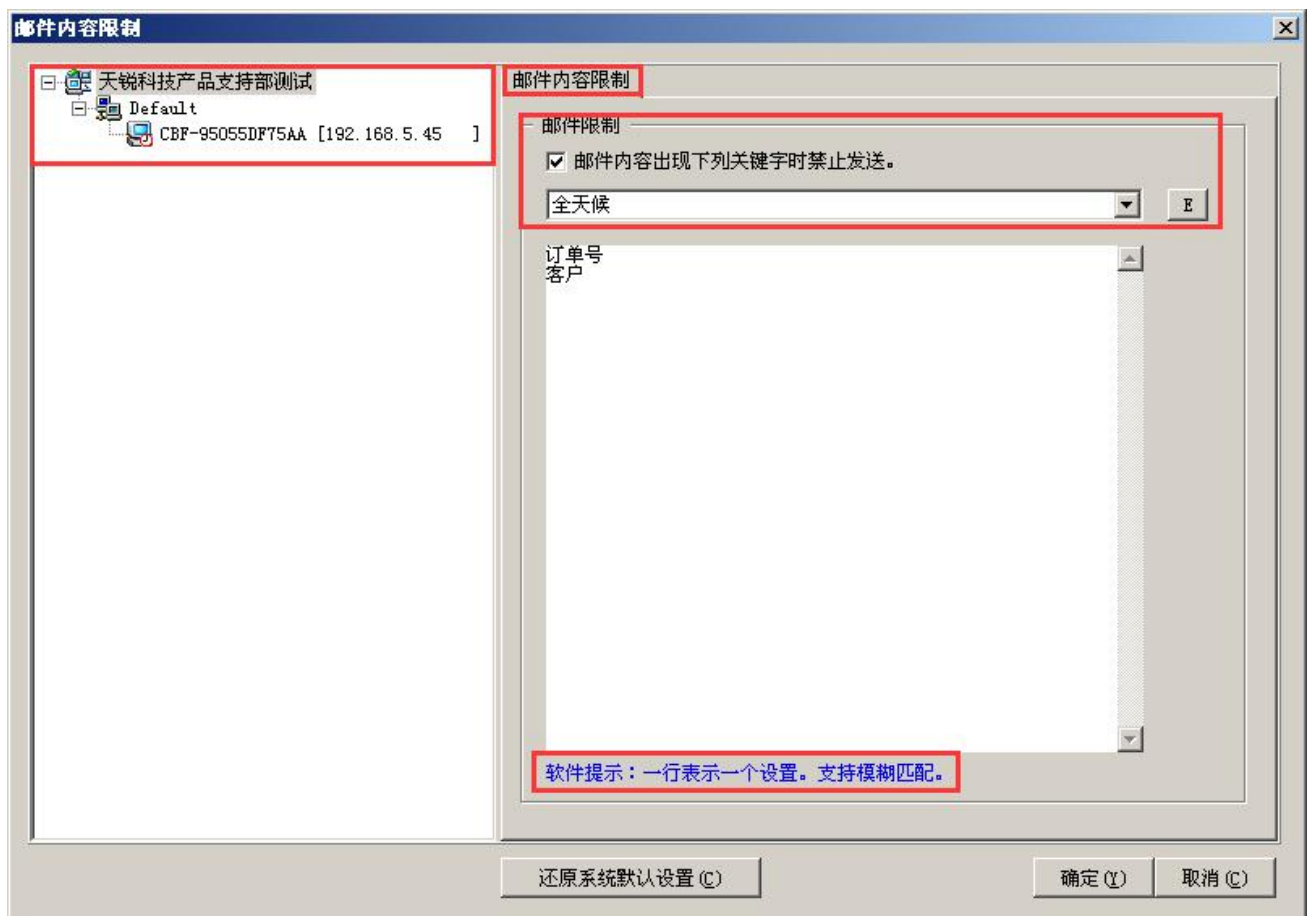
在窗口左侧选择要设置的对象（可以选择公司名称、分组或终端），在窗口右侧先勾选要分配的策略，然后在“违规控制”栏中进行违规选项设置，选项包括告警管理端（管理人员）、管理端不弹出报警信息提示、断开违规网络。配置时要记得勾选界面右上方的“策略配置生效”复选框，如果没有勾选该选项，则策略不会生效。策略设置完成后，点击“确定”按钮，即完成相应的网络隔离配置。

如果违规控制选项设置管理端弹出报警信息提示，则当发现终端有违规外联时，管理端将弹出如下提示窗口：



2.2.16 邮件内容限制

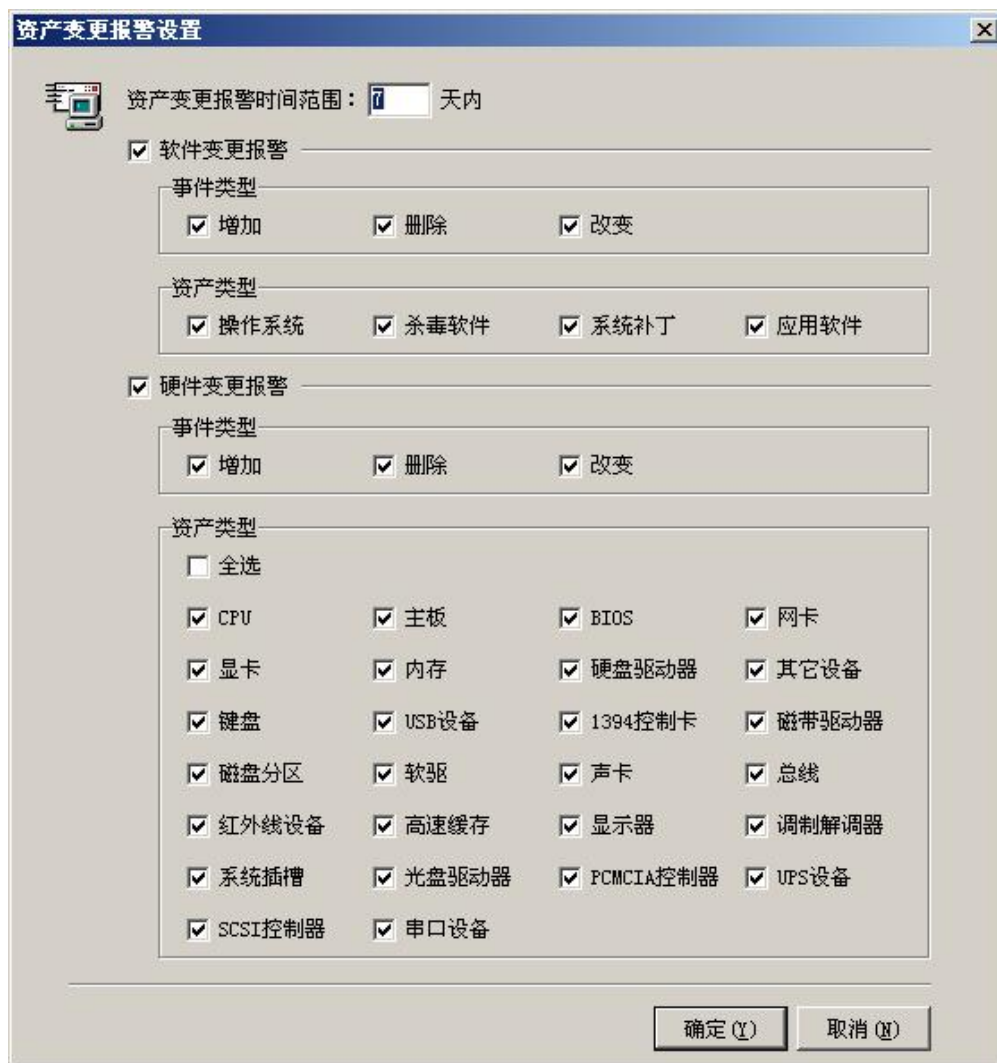
可以对终端发送的邮件内容进行限制。在控制台的功能栏选择“策略管理”-“邮件内容限制”，在弹出的“邮件内容限制”左侧选择需要限制的对象（可以选择公司名称、分组或终端），窗口右侧勾选“邮件内容出现下列关键字时禁止发送”选项，可以点击“E”按钮设置限制策略的生效时间，再在左下方输入栏中填写要限制的关键字。如下图所示：



2.3 资产管理

2.3.1 资产变更报警设置

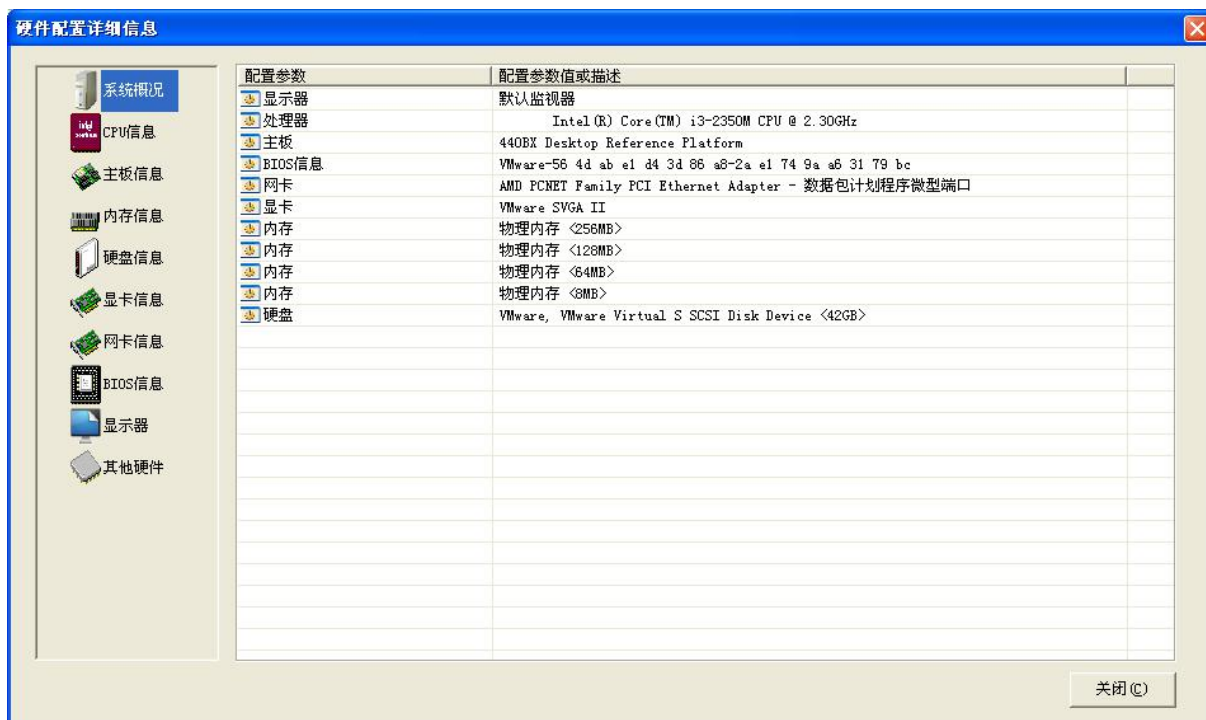
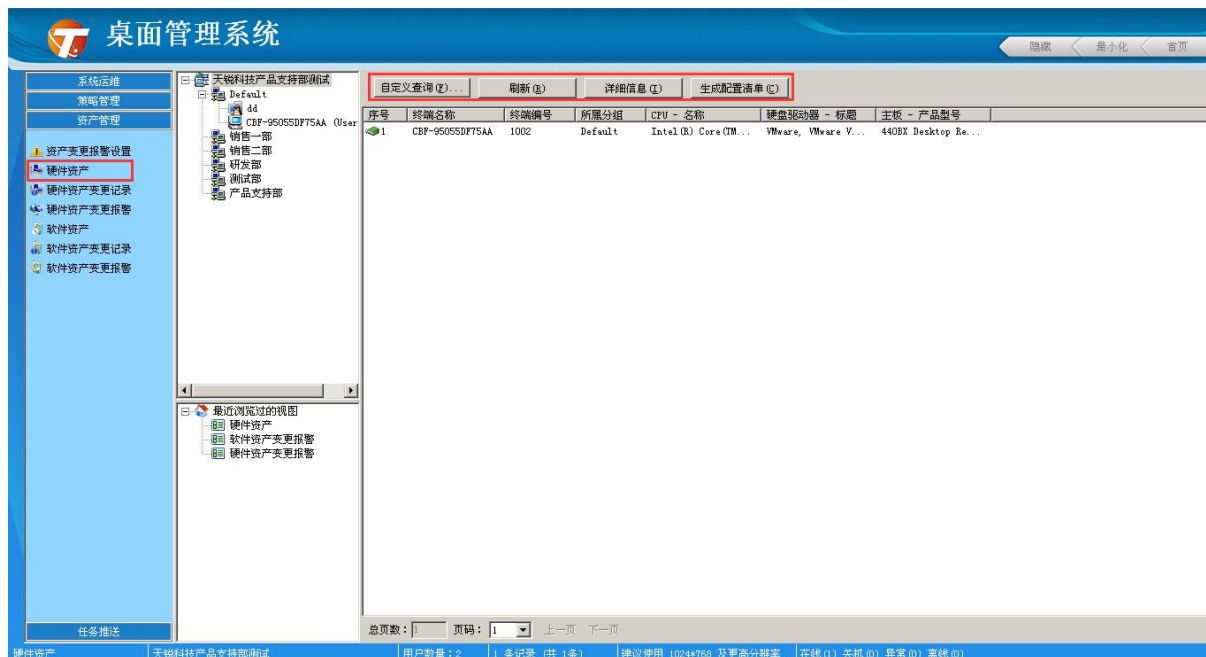
在控制台的功能栏选择“资产管理”-“资产变更报警设置”，弹出“资产变更报警设置”窗口，设置报警时间范围，勾选需要报警的事件类型和资产类型，设置完成后点击“确定”即可。如下图所示：



2.3.2 硬件资产

在控制台的功能栏选择“资产管理”-“硬件资产”，用户列表栏选中要查看的用户（可以选择公司名称、分组或终端），详细信息栏将显示选中终端电脑的硬件资产信息。系统默认查询的硬件信息包括 CPU 名称、硬盘驱动器标题、主板型号，可以点击“自定义查询”按钮

查询其他内容。双击记录或点击“详细信息”按钮，可以查看该终端的详细硬件配置。也可以把查询到的终端电脑的配置生成配置清单或导出为文件存储。如下图所示：

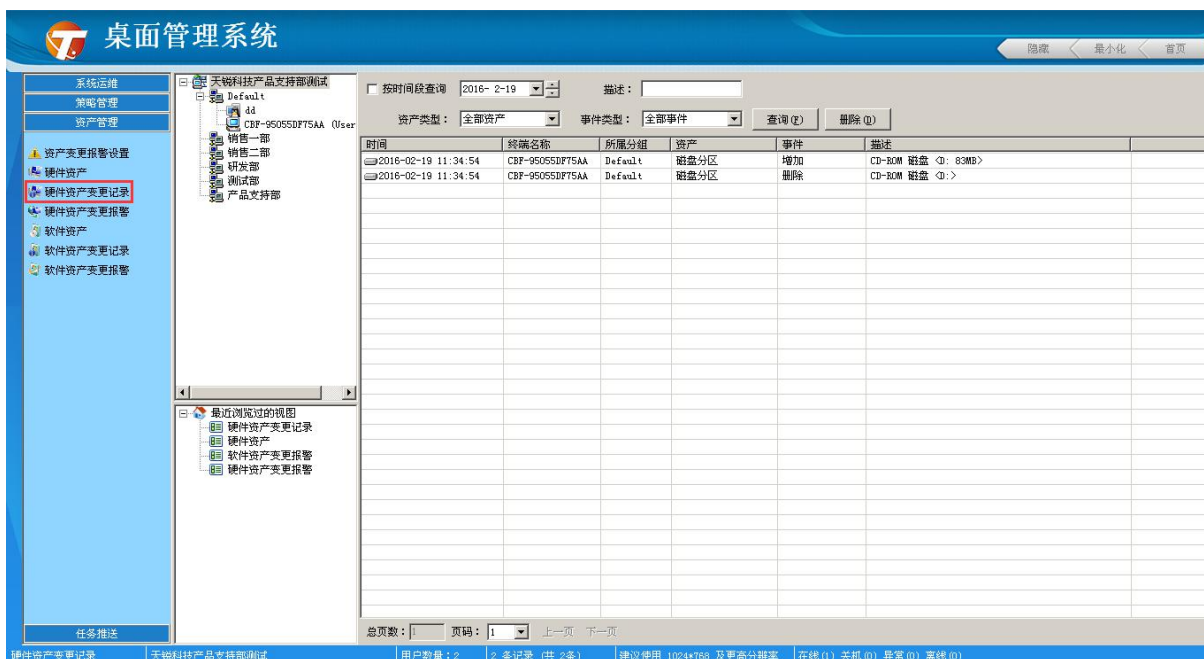


可以根据硬件或软件的名称自定义查询。如要查询局域网内有 NVIDIA 显卡的终端，可以点击“自定义查询”，在弹出的“定制资产查询条件”窗口中，点击“添加”，选择“显卡” - “名称”，填写“NVIDIA”，确定后，在主界面上即显示安装有 NVIDIA 显卡的终端。如下图所示：



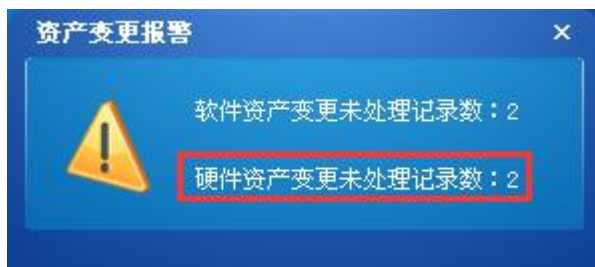
2.3.3 硬件资产变更记录

在控制台的功能栏选择“资产管理”-“硬件资产变更记录”，用户列表栏选中要查看的用户（可以选择公司名称、分组或终端），详细信息栏将显示选中终端的硬件变更情况，包括更改时间、终端名称、所属分组、资产、事件以及描述。如下图所示：

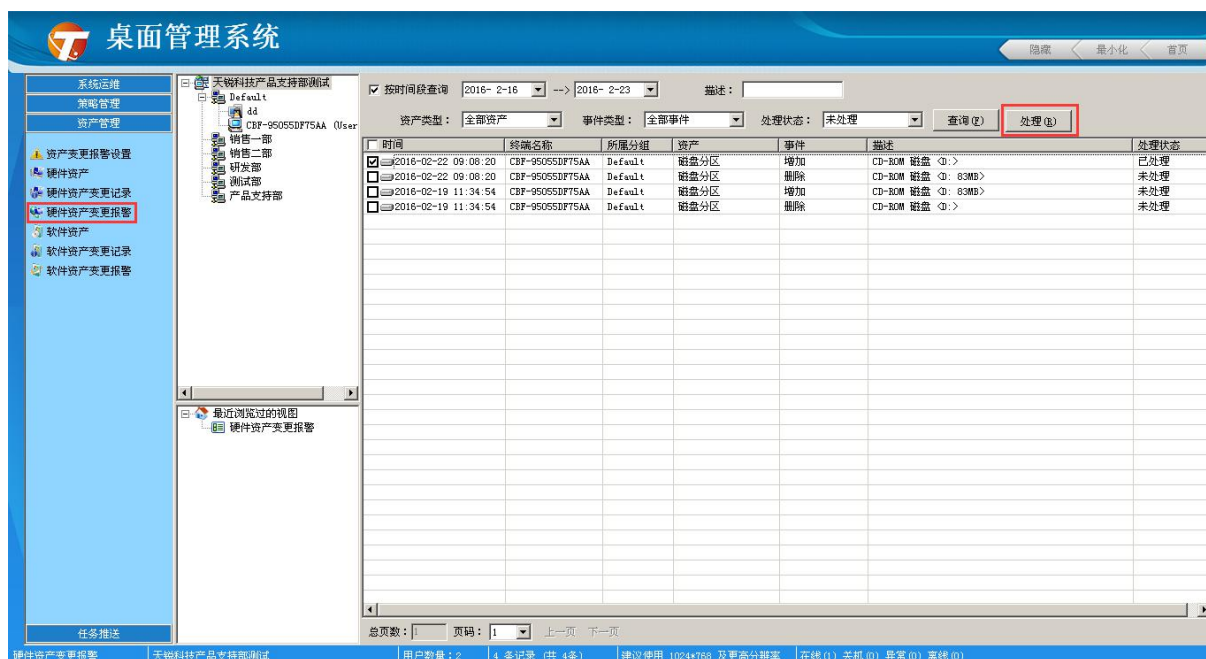


2.3.4 硬件资产变更报警

当发生硬件资产变更时，登录控制台后会弹出变更提醒窗口，如下图所示：



选择“硬件资产变更未处理记录数”跳转到“硬件资产变更提醒”界面，或者在控制台的功能栏选择“资产管理”-“硬件资产变更提醒”跳转该界面，在左侧用户列表栏选中要查看的用户（可以选择公司名称、分组或终端），详细信息栏将显示选中终端的硬件变更情况，包括更改时间、终端名称、所属分组、资产、事件、描述以及处理状态。如下图所示：



可以选择要处理的硬件变更记录，然后点击“处理”按钮，弹出“处理确认”窗口，如下图所示：



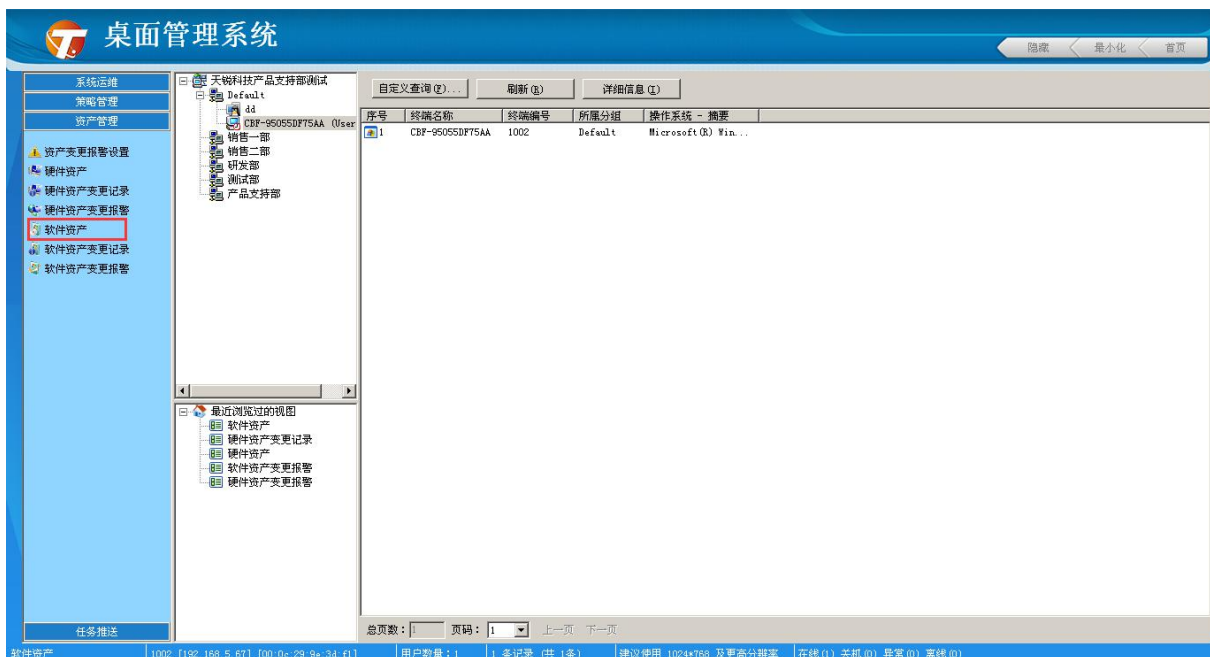
点击“确定”按钮，弹出提示，如下图所示：

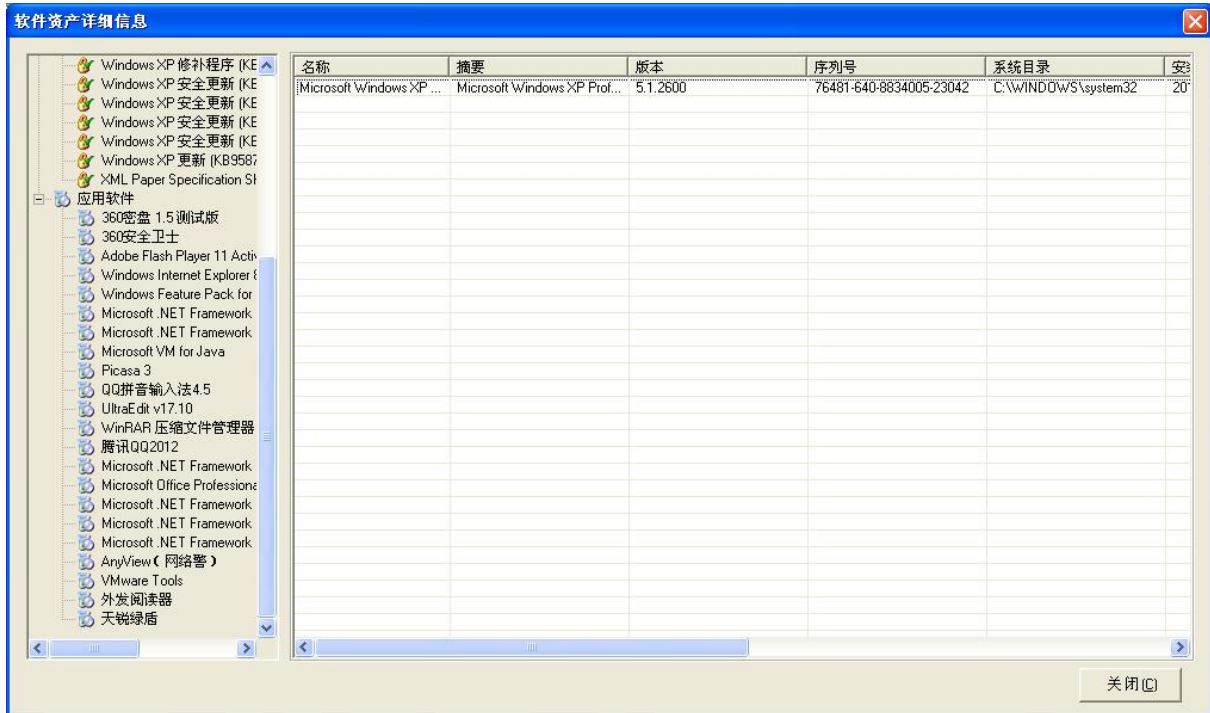


说明：下次登录控制台时已处理的变更记录不会再提醒，如未处理下次登录会继续弹出提醒框。

2.3.5 软件资产

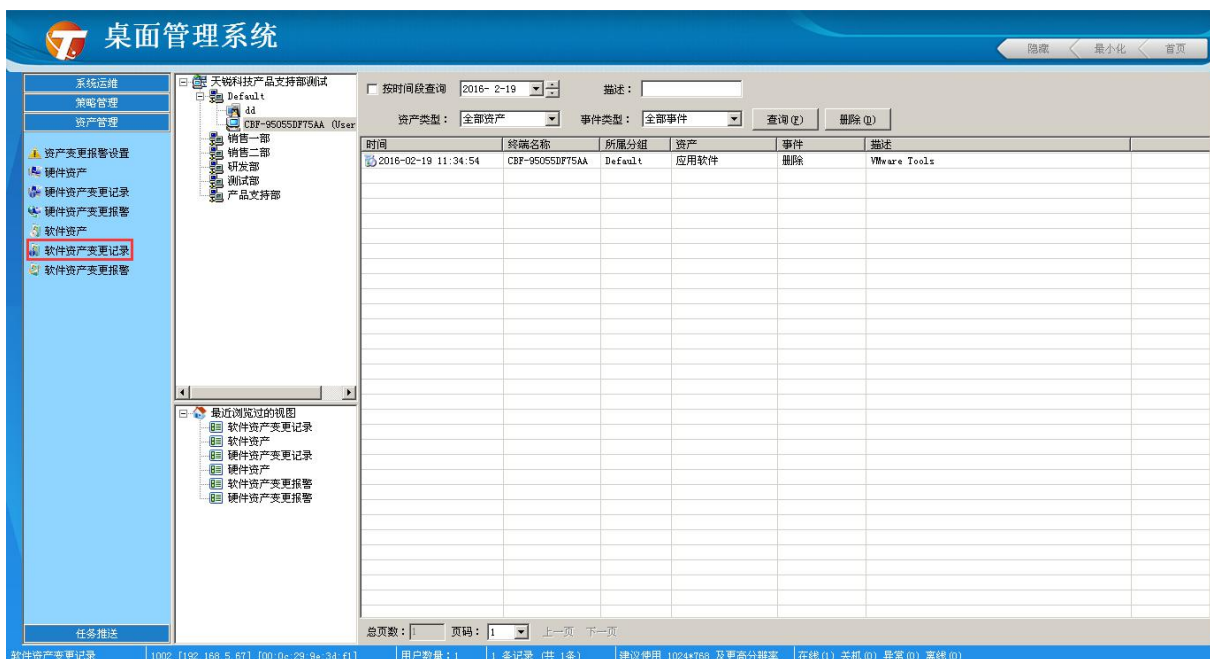
在控制台的功能栏选择“资产管理”-“软件资产”，用户列表栏选中要查看的用户（可以选择公司名称、分组或终端），详细信息栏将显示选中终端电脑的软件资产信息。系统默认查询的软件信息为操作系统，可以点击“自定义查询”按钮查询其他内容。双击记录或点击“详细信息”按钮，可以查看该终端的详细软件资产信息。如下图所示：





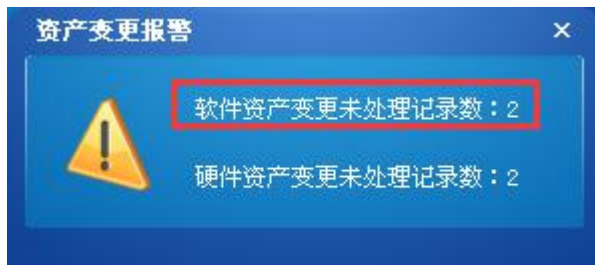
2.3.6 软件资产变更记录

在控制台的功能栏选择“资产管理”-“软件资产变更记录”，用户列表栏选中要查看的用户（可以选择公司名称、分组或终端），详细信息栏将显示选中终端的软件变更情况（安装、卸载），包括更改时间、终端名称、所属分组、事件、以及描述。如下图所示：

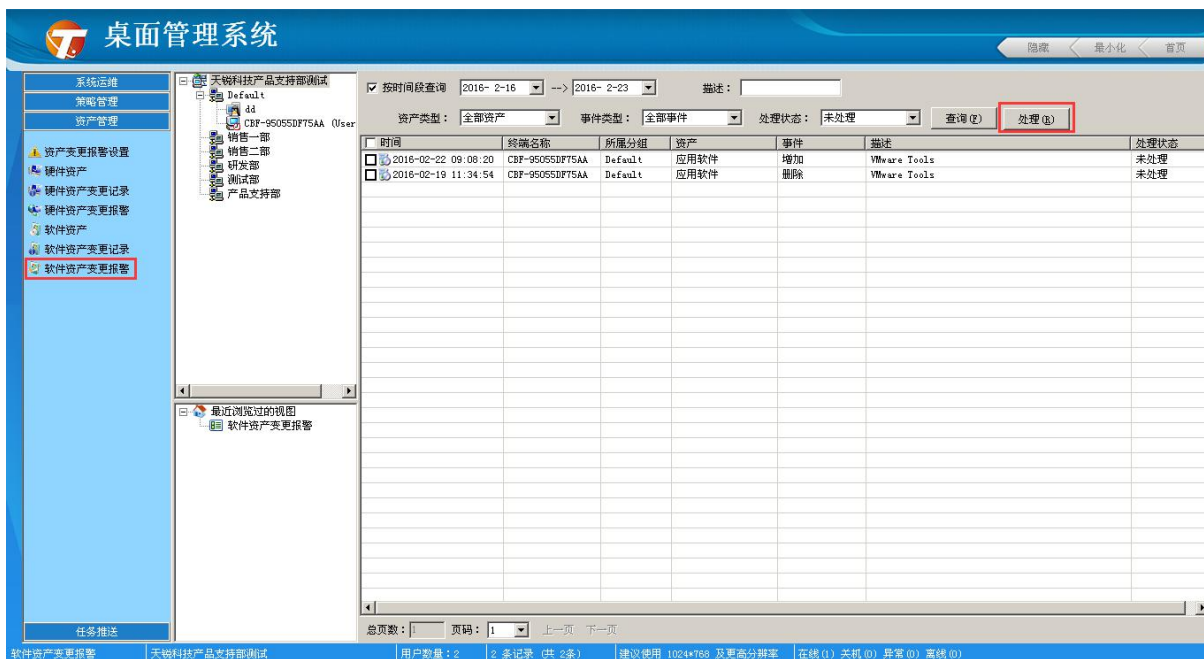


2.3.7 软件资产变更报警

当发生软件资产变更情况时，登录控制台后会弹出变更提醒窗口，如下图所示：



选择“软件资产变更未处理记录数”跳转到“软件资产变更提醒”界面，或者在控制台的功能栏选择“资产管理”-“软件资产变更提醒”跳转该界面，在左侧用户列表栏选中要查看的用户（可以选择公司名称、分组或终端），详细信息栏将显示选中终端的硬件变更情况，包括更改时间、终端名称、所属分组、资产、事件、描述以及处理状态。如下图所示：



可以选择要处理的软件资产变更记录，然后点击“处理”按钮，弹出“处理确认”窗口，如下图所示：



点击“确定”按钮，弹出提示，如下图所示：



说明：下次登录控制台时已处理的变更记录不会再提醒，如未处理下次登录会继续弹出提醒框。

2.4 任务推送

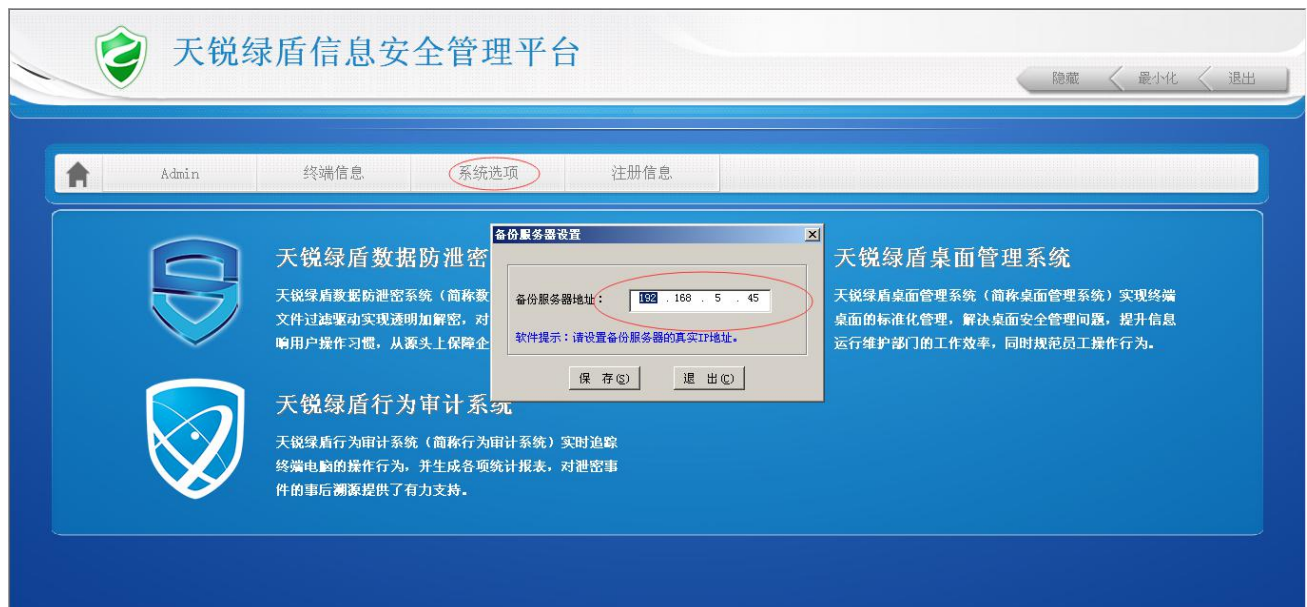
2.4.1 文件分发

向终端电脑分发文件，文件分发通过任务的方式进行，分发的文件分别为普通文件和安装文件两种类型。

2.4.1.1 上传分发文件

先配置备份服务器

在控制台首页选择“系统选项”-“备份服务器设置”，弹出“备份服务器设置”窗口，配置备份服务器地址，如下图所示：

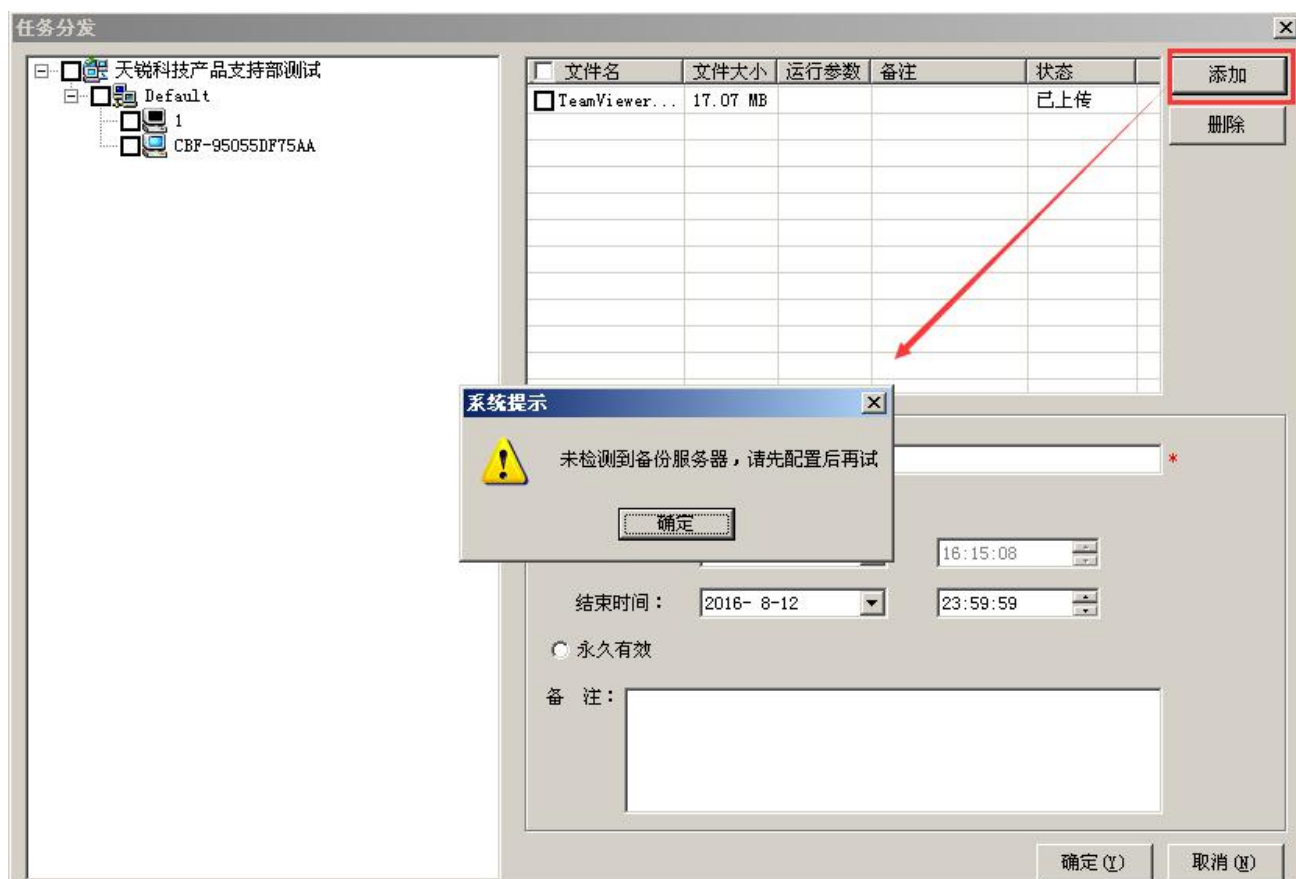


点击“添加”按钮，弹出“添加文件”窗口，首先在“文件路径”后选择“浏览”查找文件所在添加文件/文件夹，添加后文件名称会自动关联上，文件名称可以根据需要修改；然后要选择文件分发的类型，为普通文件或安装文件，还可以根据需要进行备注说明。如下图所示：



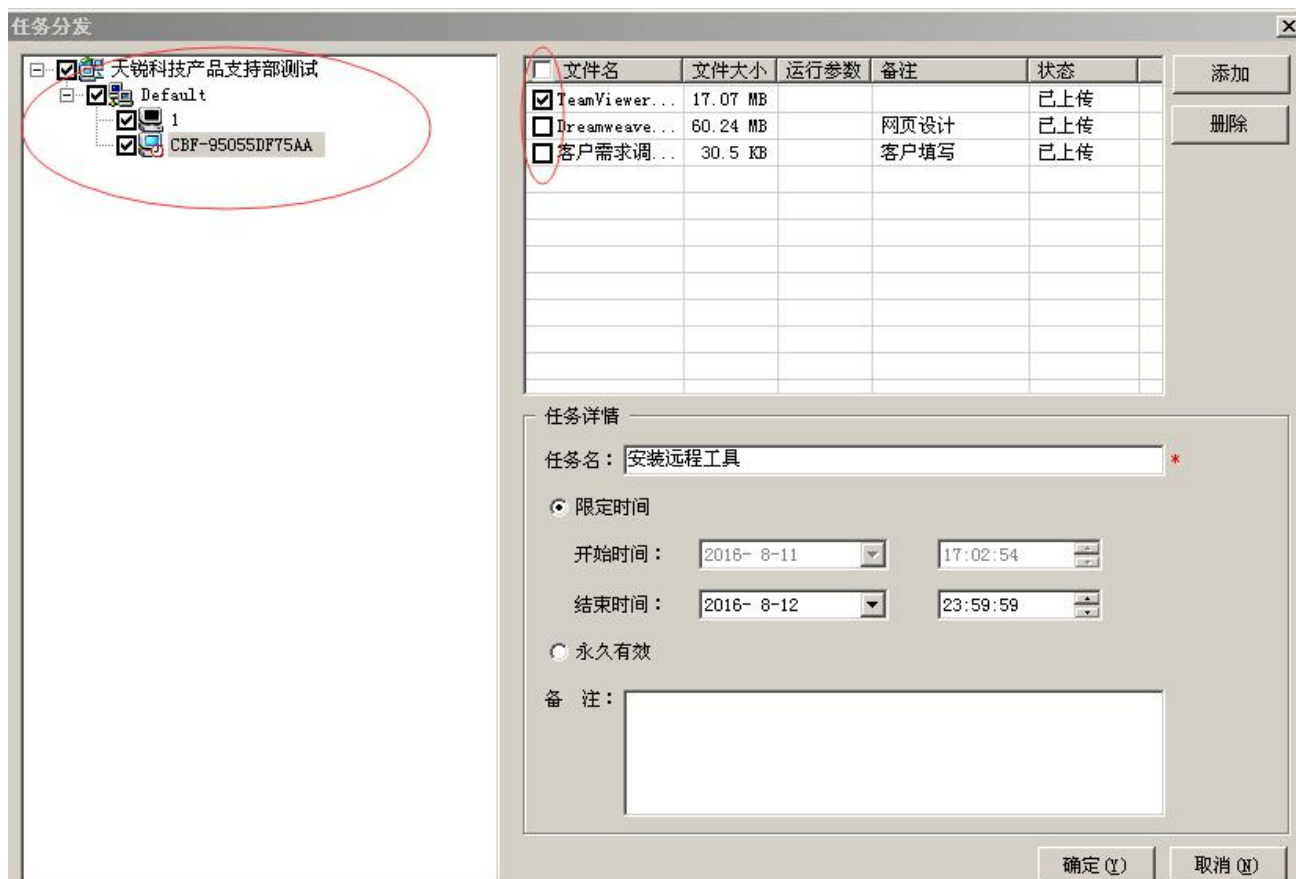
说明：如果是安装文件的话，“执行参数”栏根据需要填写，一般用于执行安装文件特定功能，与安装文件有关，没有的话就不需要填写。（如批处理文件中设置了参数，则执行参数会作为输入参数执行）

如果没有配置备份服务器的话，添加任务时会提示“未检测到备份服务器，请先配置后再试”，如下图所示：



2.4.1.2 创建并分配任务

在控制台的功能栏中选择“任务推送”-“文件分发”，弹出“文件分发”窗口，窗口左侧选择操作的用户（可以选择公司名称、分组或终端），窗口右侧上方的文件列表中选择文件，下方的任务详情中输入任务相关信息，如任务名称，任务期限以及备注，设置完成后点击确定即可。如下图所示：

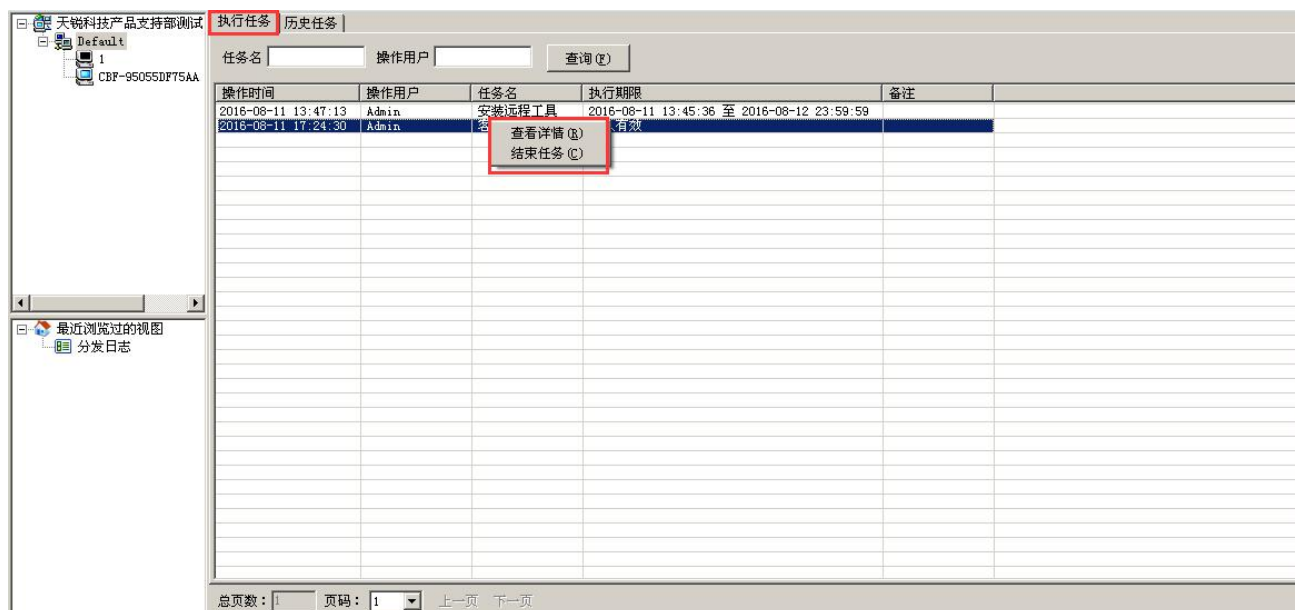


2.4.2 分发日志

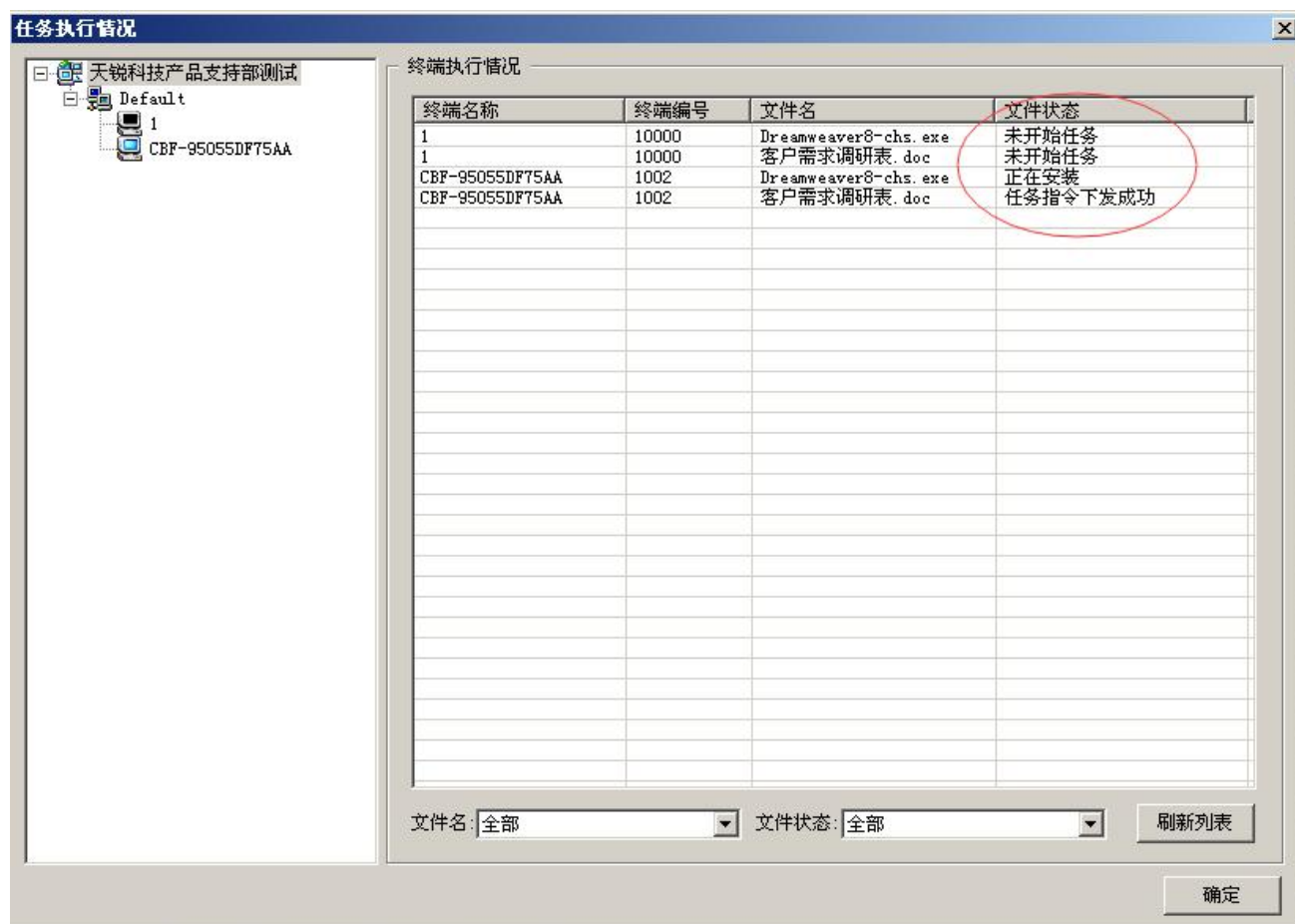
可以查看执行任务的信息，任务内容、下发以及执行情况；另外也可以查看任务的历史记录。

2.4.2.1 执行任务

在控制台的功能栏中选择“任务推送”-“分发日志”，弹出“分发日志”窗口，选择“执行任务”页面，可以查看执行任务的信息：操作时间、操作用户、任务名、执行期限和备注。还可以选择某条任务，右键鼠标查看任务详情或结束任务。如下图所示：



查看详情：选择要查看的任务，右键鼠标选择“查看详情”，弹出“任务执行情况”窗口，在窗口左侧选择要查看的对象（可以选择公司名称、分组或终端），窗口右侧查看终端执行情况，列表中分别显示终端名称、终端编号、文件名和文件状态。如下图所示：



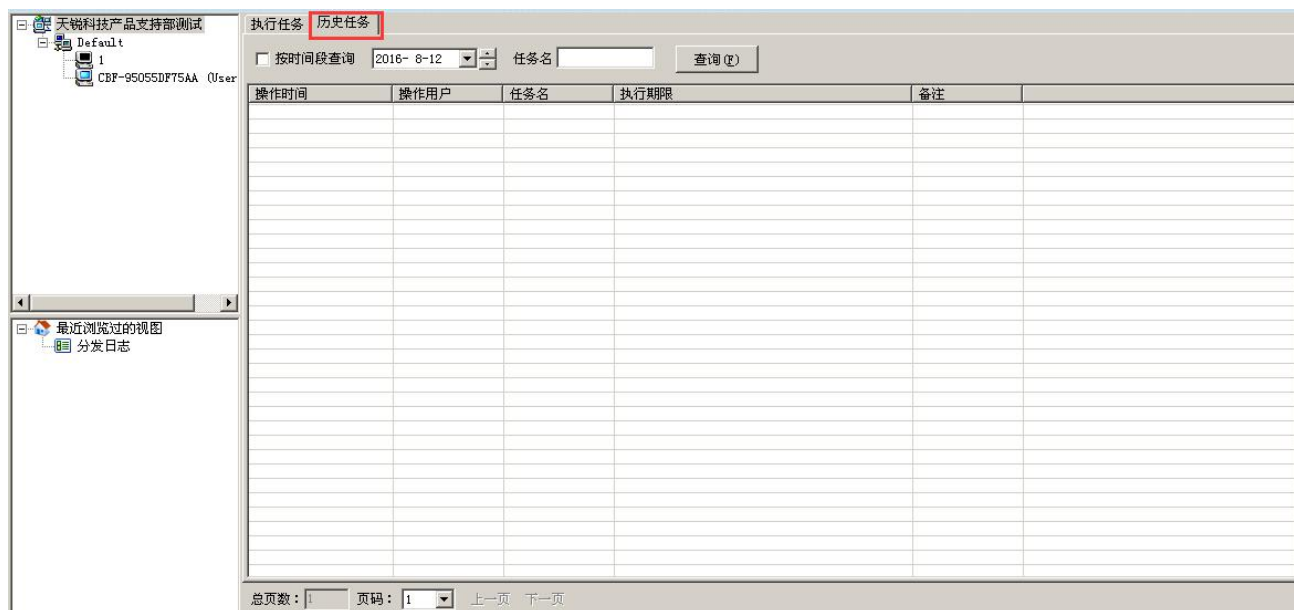
结束任务：选择要结束的任务，右键鼠标选择“结束任务”，弹出提示窗口，点击确定即

可。如下图所示：



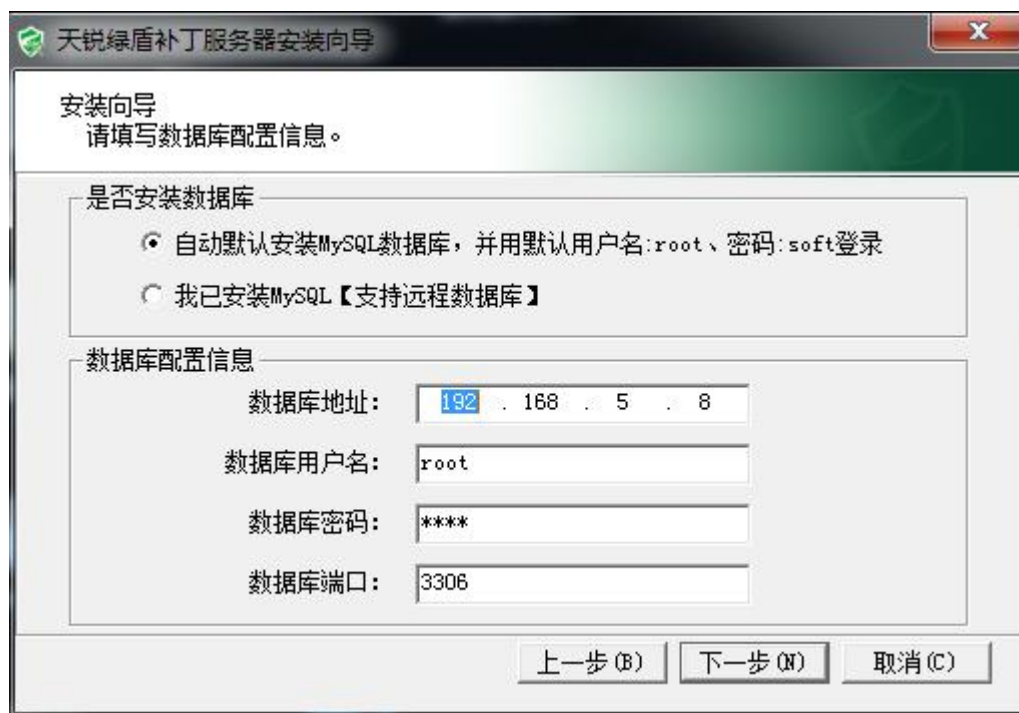
2.4.2.2 历史任务

可以根据时间、任务名来查找历史任务。在控制台的功能栏中选择“任务推送” - “分发日志”，弹出“分发日志”窗口，选择“历史任务”页面，可以查看历史任务的信息：操作时间、操作用户、任务名、执行期限和备注。



2.5 补丁管理

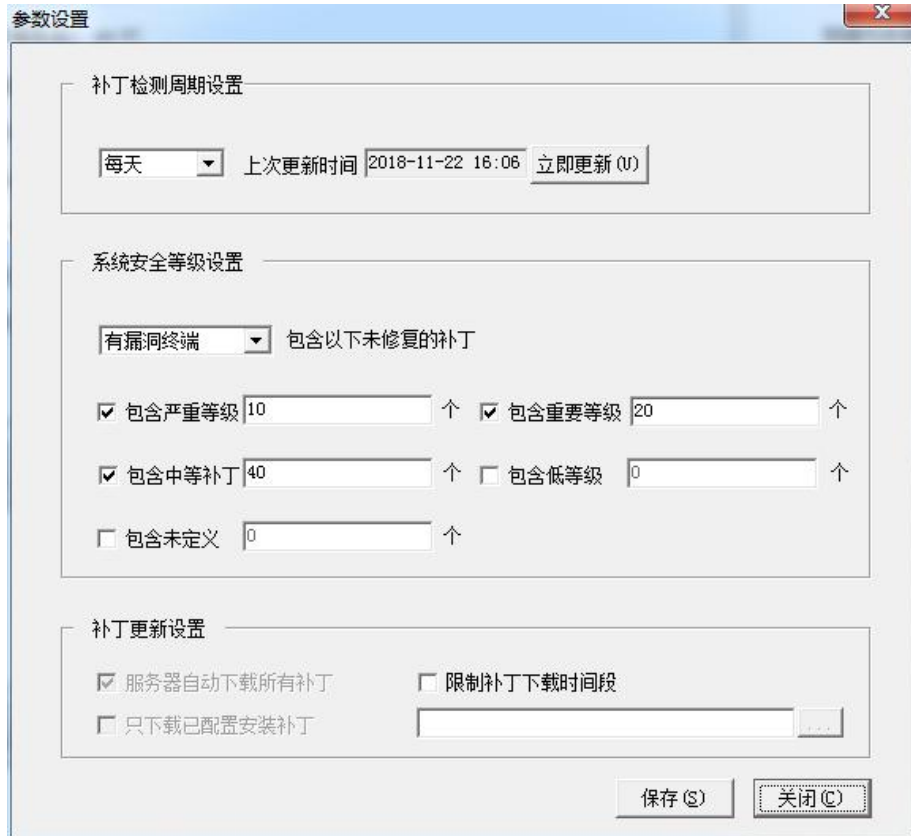
“安装补丁管理服务器”：补丁管理系统可以帮助企业集中管理、修复终端操作系统漏洞，使用补丁管理模块，需要安装补丁服务器。选择一台服务器，打开补丁管理服务器安装包，按照提示进行安装。默认安装 SQL 数据库，用户名：root，密码：soft。若已有数据库，则填写相应参数即可。



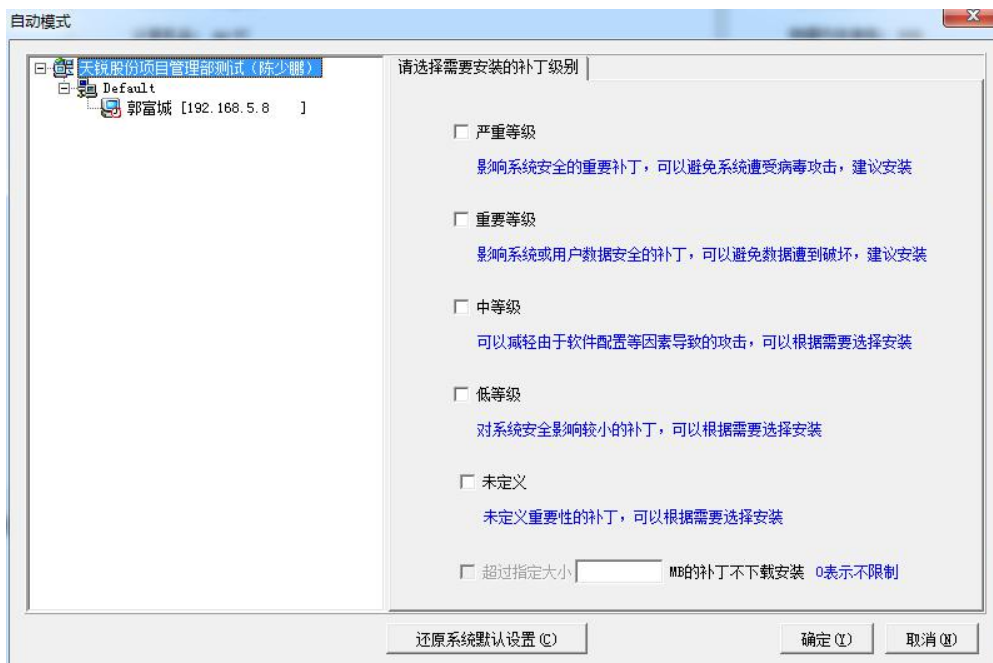
“连接绿盾引擎服务器”：完成数据参数设置后，点击“下一步”，填写绿盾引擎服务器及端口，以及本地端口（不能与现有端口冲突，一般默认即可），点击“安装”，若参数无误，即可完成安装。

“设置补丁下载参数”：完成安装后，打开绿盾控制台，依次点击：天锐绿盾桌面管理系统—补丁管理—参数设置，根据需求设置相应参数，其中“补丁管理检查周期”：补丁服务器自动到微软更新检测包的周期，可设置每天、每周或每月，第一次安装，建议点击“立即更新”。

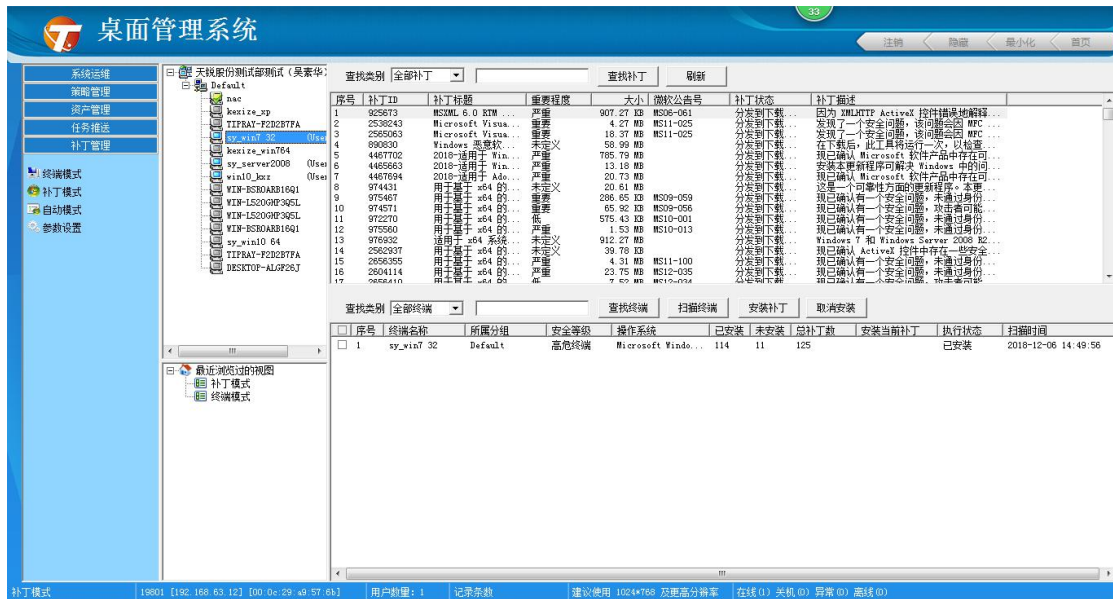
“系统安全等级设置”：可根据公司情况为终端定义等级，包括“高危终端”、“有漏洞终端”、“健康终端”。“补丁设置”：补丁下载会占用带宽及终端内存，此处可配置只下载“自动模式”中设置的补丁或只在指定的时间段下载补丁。



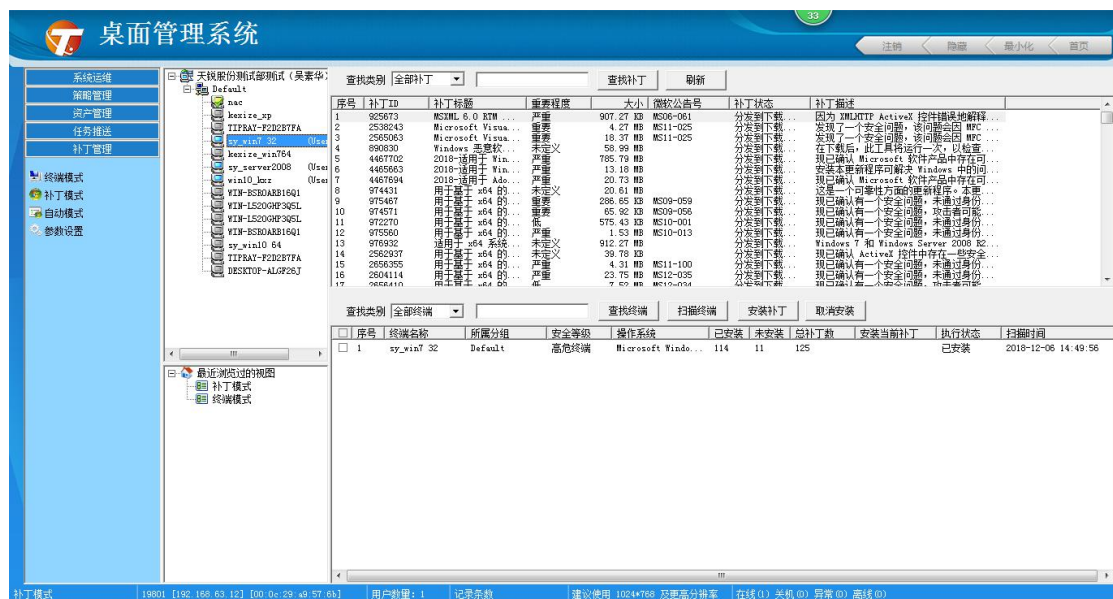
“自动模式”：可以配置指定部门或终端自动安装指定级别的补丁，其中补丁等级由微软官方定义。



“补丁模式”：将扫描结果按补丁展示，可对补丁进行优先下载管理，选择补丁可查看对应漏洞终端，可勾选终端统一安装该补丁。



“终端模式”：可选择按部门或终端执行扫描，完成扫描后，扫描结果按终端展示，并根据参数配置情况将终端划分三个等级：健康、有漏洞、高危终端。选择相应终端，可查看该终端的漏洞详情以及可以勾选相应的漏洞进行补丁安装。



“卸载补丁管理服务器”：如需卸载审批服务器，重新双击安装包或者到开始菜单中找到天锐补丁服务器并点击卸载，即可进入卸载流程。卸载后，引擎将不可使用补丁管理系统，补丁库中的补丁和相关的策略配置也将全部消失。